

Deteção e resposta a incidentes de cibersegurança

Quadro de cooperação da UE regista progressos, mas é apenas parcialmente eficaz devido a atrasos na execução e à escassa partilha de informações



Índice

Pontos

01-23 | Principais mensagens 01

01-07 | Importância deste tema

08-23 | Conclusões e recomendações

24-01 | Observações do Tribunal em pormenor 02

24-74 | As redes e os mecanismos de cibersegurança da UE apoiam a cooperação e a resposta, mas a escassa partilha de informações e a execução incompleta reduzem a sua eficácia

24-51 | As redes da UE permitem a cooperação entre Estados-Membros, mas a escassa partilha de informações reduz o seu valor acrescentado

52-61 | A Reserva de Cibersegurança da UE permite a mobilização rápida de serviços de resposta a incidentes

62-74 | O Sistema Europeu de Alerta em matéria de Cibersegurança visa melhorar as capacidades de deteção de ameaças, mas não está operacional

75-01 | Os projetos financiados pela UE no âmbito do programa DIGITAL visam reforçar a cibersegurança, mas enfrentam dificuldades na execução e na comunicação de informações

75-81 | Os atrasos na criação da Comunidade de Competências em Cibersegurança impediram-na de adaptar o programa DIGITAL às suas necessidades

82-96 | Os projetos financiados pela UE visam objetivos pertinentes, mas muitos enfrentam problemas operacionais

97-01 | A maioria dos projetos financiados pela UE tem quadros de desempenho inadequados, e os dados do programa DIGITAL sobre o desempenho em termos de cibersegurança não são exatos

Anexos

Anexo I – Sobre a auditoria

Anexo II – Panorama de cibersegurança da UE

Anexo III – Ações de cibersegurança selecionadas

Anexo IV – Avaliação do Tribunal aos projetos de cibersegurança financiados pela UE

Siglas, acrónimos e designações abreviadas

Glossário

Respostas da Comissão

Respostas do Centro Europeu de Competências em Cibersegurança (ECCC)

Respostas da Agência da União Europeia para a Cibersegurança (ENISA)

Cronologia

Equipa de auditoria

01

Principais mensagens

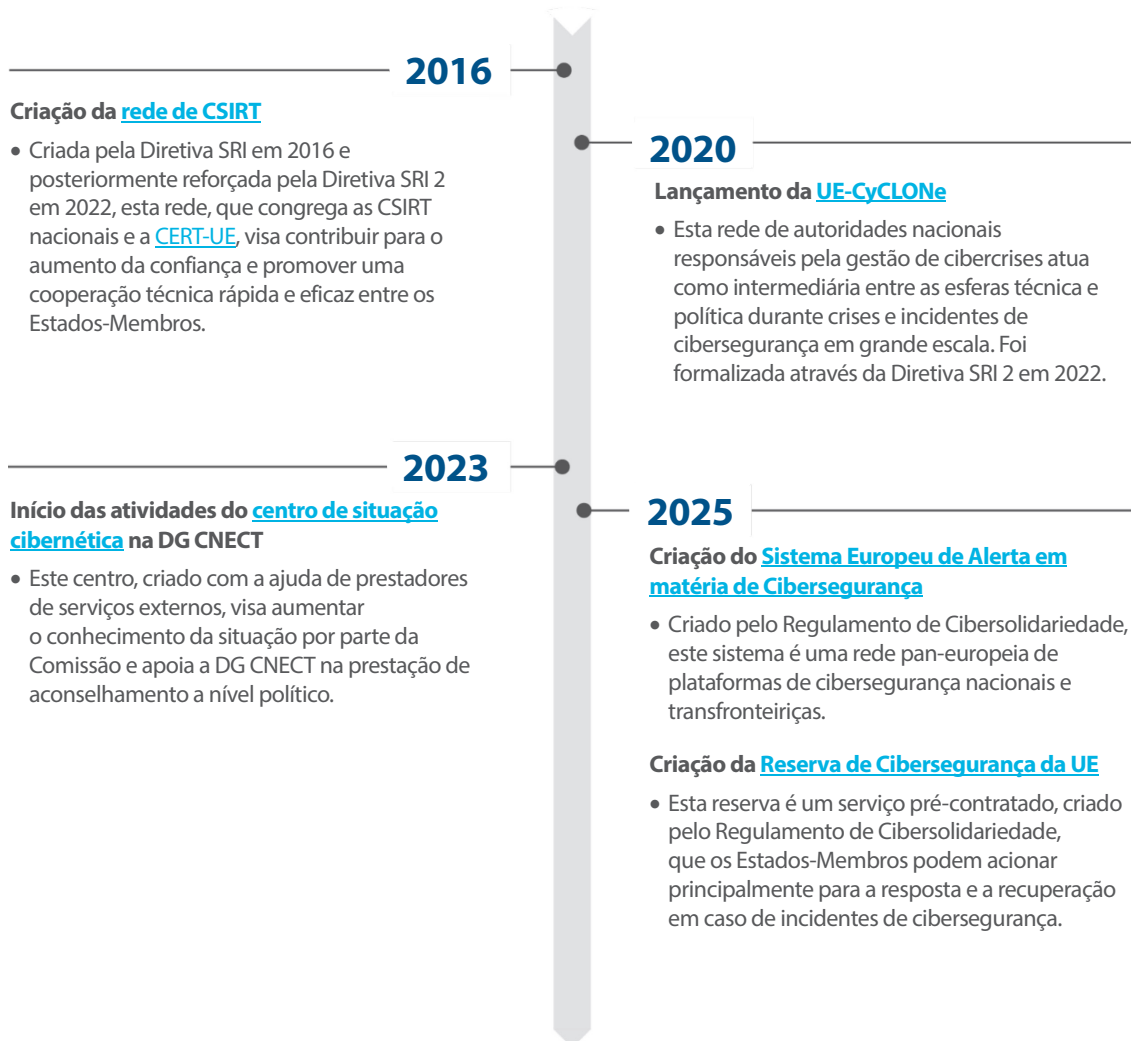
Importância deste tema

- 01** Os riscos de ciberataques aumentam à medida que a economia e a vida quotidiana se tornam mais digitalizadas. A cibersegurança é definida como "as atividades necessárias para proteger de ciberameaças as redes e os sistemas de informação, os seus utilizadores e outras pessoas afetadas"¹. Exige uma abordagem holística para prevenir e detetar ciberameaças, responder às mesmas e delas recuperar.
- 02** O panorama da cibersegurança na União Europeia (UE) envolve numerosas entidades públicas e privadas a nível regional, nacional e da UE na esfera civil. A cibersegurança é também um elemento fundamental da segurança e defesa nacionais.
- 03** Os Estados-Membros da UE são os principais responsáveis pela prevenção de incidentes e crises de cibersegurança que os afetem, pela preparação para os mesmos e pela resposta a dar-lhes. Uma vez que estes incidentes podem prejudicar o bom funcionamento do mercado interno, a União também desempenha um papel importante em caso de crise ou incidente significativo. Nos últimos anos, a UE reforçou o seu quadro regulamentar em matéria de cibersegurança², que está em constante evolução, e criou redes e mecanismos, como ilustrado na [Figura 1](#) e no [Anness II](#).

¹ [Regulamento \(UE\) 2019/881](#) (Regulamento Cibersegurança).

² Por exemplo, a Comissão propôs o [Regulamento Omnibus Digital](#) em novembro de 2025 e uma [revisão do Regulamento Cibersegurança](#) em janeiro de 2026.

Figura 1 | Redes e mecanismos de cibersegurança da UE, 2016-2025



CSIRT: Equipas de Resposta a Incidentes de Segurança Informática

DG CNECT: Direção-Geral das Redes de Comunicação, Conteúdos e Tecnologias

UE-CyCLONe: Rede Europeia de Organizações de Coordenação de Cibercrises

Diretiva SRI: 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

Diretiva SRI 2: Diretiva (UE) 2022/2555 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União

Fonte: TCE.

- 04** Ao abrigo do quadro financeiro plurianual para 2021-2027, a principal fonte de financiamento da cibersegurança é o [Programa Europa Digital](#) (DIGITAL). O seu orçamento total é de 8,1 mil milhões de euros, dos quais 1,4 mil milhões de euros se destinam ao reforço da cibersegurança.

- 05** O Tribunal realizou a presente auditoria para avaliar se as ações da UE são eficazes a facilitar a detecção de incidentes de cibersegurança significativos e em grande escala e a resposta aos mesmos. Verificou se foi esse o caso em relação:
- às redes e aos mecanismos ao nível da UE (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; o Sistema Europeu de Alerta em matéria de Cibersegurança; o centro de situação cibernética; e a Reserva de Cibersegurança da UE);
 - às ações financiadas pelo programa DIGITAL.
- 06** As conclusões do Tribunal deverão contribuir para reforçar a ciber-resiliência da UE, melhorando a eficácia e eficiência das redes e dos mecanismos da União, bem como a seleção e o acompanhamento das ações financiadas pela UE.
- 07** A auditoria abrange o período decorrido entre 2022 e 2025. Baseia-se numa análise dos documentos pertinentes, em visitas de auditoria a três Estados-Membros (Irlanda, Grécia e Itália) e em questionários escritos e entrevistas com partes interessadas pertinentes. O [anexo I](#) apresenta mais informações de contexto e pormenores sobre o âmbito e método da auditoria.

Conclusões e recomendações

- 08** De modo geral, o Tribunal conclui que as ações da UE só em parte facilitam a detecção de incidentes de cibersegurança significativos e em grande escala e a resposta aos mesmos. Tem sido desenvolvido gradualmente um quadro de cooperação, mas os trabalhos para conseguir concluí-lo ainda estão em curso. A escassa partilha de dados, as insuficiências na comunicação de informações e os atrasos consideráveis na execução impedem as redes e os mecanismos da UE de atingirem todo o seu potencial. Os projetos financiados pelo programa DIGITAL visam objetivos pertinentes, mas muitos enfrentam problemas operacionais e atrasos e há insuficiências no quadro global de acompanhamento do desempenho.

- 09** O atual quadro de redes e mecanismos da UE para facilitar a deteção de incidentes de cibersegurança significativos e a resposta aos mesmos foi desenvolvido gradualmente. Em 2025, o Conselho adotou o [Plano de Ação para a Cibersegurança](#) e estabeleceu o quadro da União para a gestão de cibercrises. O Tribunal constatou que este plano clarifica, em grande medida, as funções e responsabilidades no que diz respeito à gestão de cibercrises na UE. Não obstante, ainda não foi formalizado um método para a rede de CSIRT (criada em 2016) e a UE-CyCLONe (oficializada em 2023) trabalharem em conjunto (ver pontos [24](#) a [30](#)).
- 10** O Tribunal constatou que é escassa a partilha de informações através destas redes. Os principais motivos são atrasos na transposição da [diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União](#) (Diretiva SRI 2), dificuldades em determinar se um incidente tem impacto transfronteiriço e legislação nacional em matéria de segurança que restringe a partilha de informações. O valor acrescentado das redes reduz-se bastante se os Estados-Membros não estiverem dispostos a partilhar informações oportunas e práticas (ver pontos [31](#) a [44](#)).



Recomendação 1

Aumentar a partilha de informações entre Estados-Membros

De forma a melhorar a deteção de incidentes de cibersegurança e a resposta aos mesmos, a Comissão, com o apoio da Agência da União Europeia para a Cibersegurança (ENISA), deve:

- a) propor ao grupo de cooperação para a segurança das redes e da informação que realize uma análise pormenorizada das restrições de segurança nacional que limitam a partilha de informações e afetam a ciber-resiliência da UE e que aponte soluções jurídicas e técnicas para aumentar essa partilha sem desrespeitar os limites de segurança nacional;
- b) sem prejuízo das decisões dos legisladores, assegurar, em colaboração com os Estados-Membros, que o ponto de entrada único para a comunicação de incidentes proposto pelo Regulamento *Omnibus* Digital possa detetar eventuais incidentes transfronteiriços;
- c) trabalhar em soluções para permitir a comunicação de incidentes em tempo real à ENISA.

Prazo de execução: a) e b), 2027; c), 2028

- 11** Em 2022, a Comissão criou um "centro de situação cibernética" para aumentar o seu conhecimento da situação e apoiá-la nas suas responsabilidades institucionais na gestão de crises. O funcionamento do centro assenta, em grande medida, num contrato com prestadores de serviços externos. O Tribunal constatou que o trabalho realizado por estes prestadores duplica parcialmente a capacidade existente da Agência da União Europeia para a Cibersegurança (ENISA) no que diz respeito ao conhecimento da situação e ao acompanhamento das ameaças. O Tribunal considera que a forma como este centro foi criado não tirou proveito suficiente do potencial de racionalização, não utilizando as informações que a Comissão e a ENISA já tinham disponíveis. Além disso, a ausência de um plano abrangente e pormenorizado para o futuro após o termo do contrato constitui um risco para o funcionamento do centro após 2026 (ver pontos [45](#) a [51](#)).



Recomendação 2

Racionalizar as capacidades da UE quanto ao conhecimento da situação em matéria de cibersegurança e otimizar a divulgação de informações

Para aumentar a eficiência, a Comissão, em colaboração com a ENISA, deve avaliar a viabilidade da aquisição e análise de informações em conjunto tendo em vista o conhecimento da situação. Deve também disponibilizar estas informações e os relatórios conexos sobre ciberameaças a todos os serviços e agências pertinentes da UE.

Prazo de execução: 2027

- 12** O [Regulamento de Cibersolidariedade](#), de 2024, cria a Reserva de Cibersegurança da UE, que visa apoiar os Estados-Membros na resposta a incidentes graves de cibersegurança e na recuperação dos mesmos. A Reserva é composta por prestadores de serviços selecionados para cada Estado-Membro, com capacidade para responderem a incidentes a qualquer hora. Embora esta estratégia ajude a dar resposta aos requisitos específicos dos Estados-Membros e a criar confiança, o orçamento disponível é repartido equitativamente entre eles e não tem em conta as necessidades específicas de cada um (ver pontos [52](#) a [57](#)).

- 13** O Tribunal considera que o recurso a prestadores pré-contratados permite a mobilização rápida de serviços de resposta a incidentes. A Reserva de Cibersegurança da UE visa principalmente apoiar a resposta e a recuperação. Porém, quando não está a ser usada para a resposta a incidentes, pode ser utilizada para a preparação. Esta flexibilidade pode evitar que os serviços pré-pagos não sejam utilizados. Porém, existe o risco de a Reserva ser utilizada sobretudo para a preparação e não para a resposta, contrariamente à finalidade prevista (ver pontos [58](#) a [61](#)).
- 14** O Sistema Europeu de Alerta em matéria de Cibersegurança é uma rede de plataformas de cibersegurança nacionais e transfronteiriças que procura melhorar a deteção e a análise de ciberameaças e a resposta às mesmas. O Tribunal constatou que, devido a atrasos consideráveis na aquisição de ferramentas e serviços, à data da auditoria as duas plataformas (ATHENA e ENSOC) ainda não estavam operacionais e que o referido Sistema ainda não estava a funcionar (ver pontos [62](#) a [70](#)).
- 15** Um dos principais objetivos do Sistema Europeu de Alerta em matéria de Cibersegurança é incentivar a partilha de informações significativas entre polos de Estados-Membros. Embora este possa resolver algumas das questões relacionadas com essa partilha, é também muito difícil integrar as plataformas de cibersegurança no já complexo panorama neste domínio. O Tribunal constatou que ainda não existem acordos de cooperação, uma taxonomia comum e normas de interoperabilidade, elementos necessários para o pleno funcionamento do Sistema (ver pontos [71](#) a [74](#)).



Recomendação 3

Integrar o Sistema Europeu de Alerta em matéria de Cibersegurança no panorama de cibersegurança da UE

A Comissão, juntamente com a ENISA e os Estados-Membros, deve assegurar a existência de mecanismos de cooperação e normas de interoperabilidade para facilitar a partilha de informações entre as plataformas transfronteiriças que fazem parte do Sistema Europeu de Alerta em matéria de Cibersegurança, da rede de CSIRT e da UE-CyCLONe.

Prazo de execução: 2028

- 16** Em 2018, a Comissão propôs a criação do Centro Europeu de Competências em Cibersegurança (ECCC) para gerir a componente de cibersegurança do programa DIGITAL a partir de 2021. O [Regulamento ECCC](#) estipulou a criação da Comunidade de Competências em Cibersegurança, composta por representantes da indústria e de organizações académicas e de investigação. Alguns membros desta Comunidade são selecionados para formar o Grupo Consultivo Estratégico (ver pontos [75](#) a [76](#)).
- 17** O Tribunal constatou que houve atrasos na concretização da autonomia financeira do ECCC e na criação da Comunidade de Competências em Cibersegurança e do Grupo Consultivo Estratégico, o que impediu a Comunidade e o Grupo de darem os seus contributos para moldar os planos de trabalho do programa DIGITAL. O Tribunal considera que esta foi uma oportunidade perdida (ver pontos [77](#) a [81](#)).
- 18** O Tribunal constatou que todos os projetos examinados prosseguiram objetivos pertinentes que ajudavam a concretizar os objetivos do programa DIGITAL em matéria de cibersegurança. Contudo, observou casos em que a qualidade ou os resultados alcançados não eram satisfatórios, sobretudo devido a atrasos na execução (ver pontos [82](#) a [87](#)).
- 19** O [regulamento relativo ao programa DIGITAL](#) prevê que, por razões de segurança, o financiamento da cibersegurança pode ser limitado a entidades estabelecidas nos Estados-Membros e controladas pelos Estados-Membros ou pelos seus cidadãos. O serviço central de validação que funciona na [Agência de Execução Europeia da Investigação](#) avalia estas questões da propriedade e do controlo em nome do ECCC (ver pontos [88](#) a [91](#)).

- 20** No caso do apoio financeiro a terceiros, a responsabilidade pela avaliação da propriedade e do controlo incumbe aos beneficiários do projeto, com base nas suas próprias estratégias e metodologias. O Tribunal constatou que o ECCC não valida estas metodologias nem realiza verificações para assegurar que a propriedade e o controlo dos terceiros selecionados se encontram na UE. Considera que existe um risco significativo de os beneficiários não terem capacidade para realizar adequadamente estes controlos. Este risco não foi devidamente atenuado e pode deixar expostos elementos sensíveis, como infraestruturas, dados operacionais e tecnologias de importância crítica para a segurança (ver pontos [92](#) a [96](#)).



Recomendação 4

Assegurar uma sólida avaliação da propriedade e do controlo das entidades que recebem financiamento da UE ao abrigo do Programa Europa Digital

O Centro Europeu de Competências em Cibersegurança deve:

- a) obter garantias razoáveis de que os beneficiários responsáveis pela prestação de apoio financeiro a terceiros têm a capacidade administrativa e técnica necessária para realizar avaliações adequadas da propriedade e do controlo, com base na metodologia disponível para os beneficiários que executam esse apoio;
- b) verificar, por amostragem, se apenas as entidades elegíveis receberam financiamento da UE.

Prazo de execução: a), 2026; b), 2027

- 21** Os beneficiários que gerem projetos financiados pela UE devem comunicar os progressos e resultados ao ECCC utilizando etapas intermédias e prestações concretas. Estes elementos são essenciais para o acompanhamento dos projetos e devem ser definidos de forma adequada. O Tribunal constatou que quase nenhum dos projetos incluídos na amostra seguiu as instruções sobre a forma de elaborar etapas intermédias e prestações concretas e que muitas não eram úteis para acompanhar os progressos realizados (ver pontos [97](#) a [99](#)).
- 22** O Tribunal constatou que muitos dos indicadores de desempenho utilizados pelos beneficiários não são pertinentes nem mensuráveis e carecem de uma meta ou de uma base de referência. Além disso, a comunicação de informações sobre estes indicadores era inadequada e, por isso, não pode servir de base para avaliar o desempenho dos projetos (ver pontos [100](#) a [102](#)).

- 23** Para acompanhar as concretizações do programa DIGITAL no seu conjunto, todos os projetos devem comunicar informações sobre indicadores específicos dos programas, que contribuem para as [declarações de desempenho sobre o programa](#) apresentadas anualmente pela Comissão. A responsabilidade pela recolha e verificação dos dados proporcionados por estes indicadores cabe ao ECCC. O Tribunal detetou vários problemas quanto à forma de recolha dos dados e à sua qualidade global. Não encontrou provas de que a exatidão dos dados comunicados tenha sido verificada pelo ECCC. Com base nos seus controlos por amostragem, o Tribunal considera que os dados comunicados não refletem com exatidão os resultados alcançados (ver pontos [103](#) a [106](#)).



Recomendação 5

Reforçar o quadro de acompanhamento do desempenho relativo à componente de cibersegurança do Programa Europa Digital

De forma a permitir um acompanhamento adequado dos progressos e do desempenho, o Centro Europeu de Competências em Cibersegurança deve:

- a) assegurar que, antes da assinatura das subvenções, todos os projetos definiram etapas intermédias, prestações concretas e indicadores de desempenho que cumpram as instruções do formulário de candidatura;
- b) conceber e aplicar um sistema sólido de recolha, rastreabilidade, verificação e agregação dos dados a utilizar nos indicadores de desempenho relativos à componente de cibersegurança do Programa Europa Digital, de modo a garantir que os indicadores refletem com exatidão os resultados alcançados.

Prazo de execução: 2027

Observações do Tribunal em pormenor

As redes e os mecanismos de cibersegurança da UE apoiam a cooperação e a resposta, mas a escassa partilha de informações e a execução incompleta reduzem a sua eficácia

As redes da UE permitem a cooperação entre Estados-Membros, mas a escassa partilha de informações reduz o seu valor acrescentado

- 24** O atual quadro da UE de redes e mecanismos para facilitar a deteção de incidentes de cibersegurança significativos e a resposta aos mesmos foi desenvolvido gradualmente. O primeiro passo foi a [diretiva relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União](#)³ (a Diretiva SRI), que entrou em vigor em agosto de 2016. O [anexo II](#) ilustra o panorama atual na UE.

³ Diretiva (UE) 2016/1148.

As redes da UE permitem a cooperação entre Estados-Membros a nível técnico e operacional

- 25** A Diretiva SRI criou a [rede de CSIRT](#), que congrega a [CERT-UE](#) (o serviço de cibersegurança para as instituições, órgãos e organismos da União) e as CSIRT designadas pelos Estados-Membros. A finalidade desta rede é criar confiança entre as CSIRT nacionais e promover uma cooperação operacional rápida e eficaz entre os Estados-Membros.
- 26** A [UE-CyCLONe](#) foi criada em 2020 como uma rede informal de cooperação entre as autoridades nacionais responsáveis pela gestão de cibercrises. Serve de ponte entre o nível técnico em que a rede de CSIRT opera e o nível político do Conselho da União Europeia com as disposições do [Mecanismo Integrado de Resposta Política a Situações de Crise](#). A entrada em vigor da Diretiva SRI 2, em 2023, formalizou o papel da UE-CyCLONe e conferiu-lhe um mandato claro.
- 27** O Tribunal avaliou se as funções e responsabilidades destas redes ao nível da UE estão bem definidas e permitem a cooperação entre Estados-Membros.
- 28** A [ENISA](#) funciona como secretariado da rede de CSIRT e da UE-CyCLONe e fornece-lhes recursos, conhecimentos especializados, infraestruturas e as ferramentas informáticas necessárias para a cooperação e a comunicação segura para partilha de informações. No seu inquérito de satisfação às partes interessadas do início de 2025⁴, a ENISA recebeu boas pontuações pelo seu desempenho enquanto secretariado destas redes. Estas impressões positivas foram confirmadas durante as visitas de auditoria do Tribunal, em que as autoridades nacionais de cibersegurança manifestaram o seu apreço.
- 29** Em 2025, o Conselho adotou o [Plano de Ação para a Cibersegurança](#), que define as funções e responsabilidades dos principais intervenientes (incluindo a rede de CSIRT e a UE-CyCLONe) e dos mecanismos envolvidos em incidentes de cibersegurança em grande escala ou cibercrises. O Tribunal constatou que este plano clarifica, em grande medida, as funções e responsabilidades no que diz respeito à gestão de cibercrises na União e tem em conta as mudanças no panorama desde a publicação do primeiro plano em 2017. O plano define três níveis de cooperação: técnico, operacional e político. Descreve as novas redes e estruturas criadas desde 2017 (como a UE-CyCLONe, as equipas da UE de resposta rápida às ameaças híbridas e o Sistema Europeu de Alerta em matéria de Cibersegurança) e de que forma a gestão de cibercrises se deve integrar no quadro mais vasto da UE para a resposta a situações de crise.

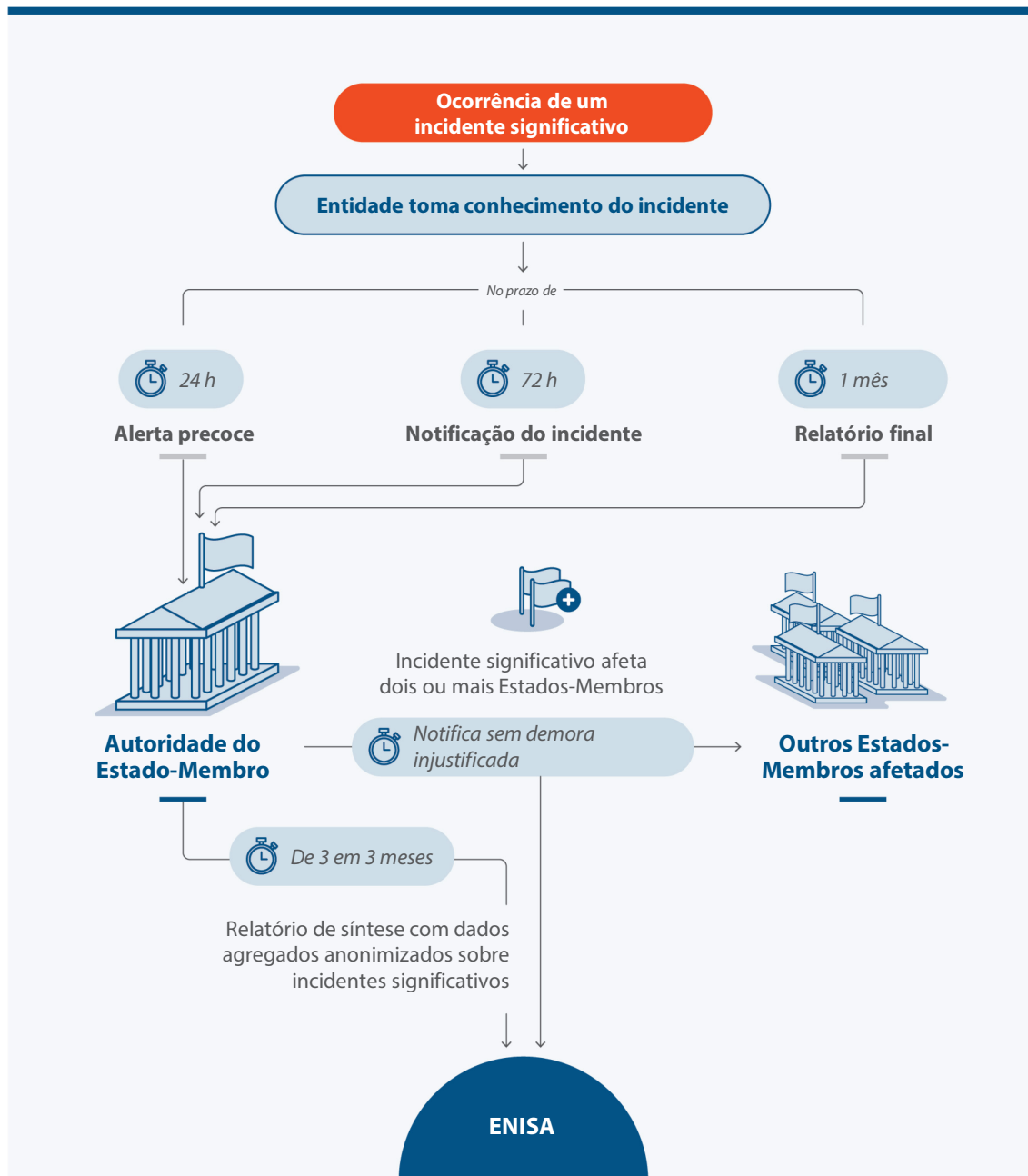
⁴ ENISA, [2024 Consolidated Annual Activity Report](#), pp. 33 e 36.

- 30** Contudo, apesar da criação oficial da rede de CSIRT em 2016 e da UE-CyCLONe em 2023, as duas redes ainda não formalizaram um método de trabalho em conjunto. Também não chegaram a acordo sobre os critérios aplicáveis para a rede de CSIRT aconselhar a UE-CyCLONe quanto à possibilidade de um incidente de cibersegurança detetado constituir um incidente de cibersegurança em grande escala, potencial ou em curso. As duas redes também têm de chegar a acordo sobre uma taxonomia comum dos níveis de gravidade dos incidentes e dos conceitos fundamentais (como "ameaça", "autor de ameaças", "incidente" ou "impacto"), que é necessária para o intercâmbio automatizado de informações. Atualmente, há margem de interpretação quanto ao momento em que um incidente é considerado significativo ou em grande escala. A falta de uma taxonomia comum foi mencionada pelas autoridades de cibersegurança dos três Estados-Membros visitados pelo Tribunal.

A escassa partilha e comunicação de informações reduz consideravelmente o valor acrescentado destas redes

- 31** As fronteiras geográficas não impedem a ocorrência e a propagação de incidentes de cibersegurança e ciberataques. A partilha de informações entre os Estados-Membros sobre, por exemplo, as táticas e técnicas utilizadas pelos autores de ameaças e sobre os sinais digitais de violação de uma rede ou de um sistema informático ("indicadores de comprometimento") pode contribuir consideravelmente para aumentar a cibersegurança.
- 32** O Tribunal constatou que havia escassa partilha de informações, reduzindo consideravelmente o valor acrescentado destas redes. As limitações observadas dizem principalmente respeito a atrasos na transposição da Diretiva SRI 2, problemas em determinar se um incidente tem impacto transfronteiriço, legislação nacional em matéria de segurança que restringe a partilha de informações e falta de confiança. A Diretiva SRI 2 introduz vários requisitos de comunicação de informações para as entidades abrangidas pelo seu âmbito de aplicação e para as autoridades dos Estados-Membros, como ilustrado na [figura 2](#).

Figura 2 | Prazos de comunicação de incidentes ao abrigo da diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na UE (Diretiva SRI 2)



Fonte: TCE, com base em dados da ENISA.

- 33** Os Estados-Membros tinham até outubro de 2024 para [transpor a Diretiva SRI 2](#) para o direito nacional, mas apenas dois cumpriram o prazo. Os atrasos na transposição têm um grande impacto na partilha de informações, na medida em que, entretanto, as entidades abrangidas pela Diretiva SRI 2 não são legalmente obrigadas a comunicar incidentes. A Comissão estimou que 15 500 entidades estavam abrangidas pela Diretiva SRI⁵, ao passo que mais de 110 000 recaem no âmbito de aplicação da Diretiva SRI 2. Por exemplo, a administração pública (o setor mais visado na UE, segundo o [relatório do estado das ameaças em 2025](#) publicado pela ENISA) não estava obrigada a comunicar incidentes ao abrigo da Diretiva SRI.
- 34** A comunicação de dados sobre incidentes à ENISA de três em três meses (ou seja, muito depois da eventual ocorrência de um incidente) diminui o valor acrescentado das informações. Estas servem principalmente para fins estatísticos e para a comunicação de tendências históricas, e não para melhorar a deteção e a resposta. A ENISA disponibiliza aos Estados-Membros uma [ferramenta online](#) para a apresentação das informações. O modelo de relatório contém um conjunto mínimo de dados a indicar, tais como o tipo de incidente e o setor em causa. Além disso, a ENISA sugere que os Estados-Membros facultem informações adicionais que permitam uma análise mais aprofundada dos dados, por exemplo associando os incidentes a vulnerabilidades específicas. Porém, nem todos os Estados-Membros optam por dar estas informações, o que reduz consideravelmente a qualidade e o valor acrescentado dos dados recolhidos.
- 35** No seu [relatório de 2024 sobre o estado da cibersegurança na UE](#), a ENISA afirmou que o número de incidentes comunicados parecia ser baixo, pelo que era provavelmente inferior ao real. Entre 2018 e 2021, os Estados-Membros comunicaram à ENISA entre 100 e 500 incidentes por ano. Este número tem vindo a aumentar gradualmente e, em 2024, chegou a 1 276⁶.

⁵ Comissão Europeia, *Impact assessment report*, 2020.

⁶ Dados do CIRAS relativos a 2024.

- 36** No seu [relatório do estado das ameaças em 2025](#), que abrange o período entre junho de 2024 e junho de 2025, a ENISA sinalizou cerca de 4 800 incidentes de cibersegurança⁷ com recurso a informações de fonte aberta, como artigos noticiosos. Nem todos estes incidentes eram passíveis de notificação ao abrigo da Diretiva SRI 2, dado que, ao recolher os dados, a ENISA abrange um leque mais vasto de situações. Em contrapartida, muitos incidentes significativos não são comunicados em informações de fonte aberta. Como os dados comunicados pelos Estados-Membros são anonimizados, a ENISA não pode conciliá-los com os incidentes que ela mesma sinaliza e, assim, não é possível determinar com precisão a diferença entre o número real de incidentes e o que é comunicado. No entanto, o Tribunal considera que a diferença entre este último e o número de incidentes referido no relatório do estado das ameaças mostra que nem todos os incidentes significativos são notificados.
- 37** Outra indicação de que há incidentes não comunicados é o número de notificações a outros Estados-Membros afetados e à ENISA acerca de incidentes transfronteiriços significativos. A Diretiva SRI já continha um requisito sobre essas notificações, mas que foi considerado ineficaz. Com efeito, a Comissão concluiu, em 2020⁸, que apesar de obrigatórias as notificações raramente eram enviadas, atribuindo a omissão à falta de modalidades claras para a partilha de informações e de objetivos comuns que incentivassem a partilha.
- 38** A obrigação de informar outros Estados-Membros é crucial para evitar a propagação de incidentes, e o seu incumprimento prejudica a cibersegurança da UE. Em 2025, foram comunicados apenas 14 incidentes transfronteiriços significativos, por sete Estados-Membros. Foram apresentados pelos Estados-Membros três relatórios de incidentes com possível impacto transfronteiriço em 2022, nenhum em 2023 e dois em 2024. Estes dados demonstram que a comunicação de incidentes transfronteiriços significativos é muito baixa e não reflete a verdadeira dimensão destes ataques. Para contextualizar a situação, no seu [relatório do estado das ameaças em 2024](#) a ENISA mencionou 322 incidentes que visavam especificamente dois ou mais Estados-Membros. O incidente com a Collins Aerospace (ver [caixa 1](#)) é um exemplo de Estados-Membros que não comunicaram um incidente, apesar de este ter um impacto transfronteiriço significativo.

⁷ [ENISA threat landscape 2025](#).

⁸ Comissão Europeia, [Impact assessment report](#), 2020.

Caixa 1

Incidente de cibersegurança que perturbou as operações aeroportuárias

Em setembro de 2025, a Collins Aerospace, um importante fornecedor de tecnologia ao setor da aviação, sofreu um ataque significativo de *ransomware* (*software* de sequestro) que visou o seu *software* de processamento de passageiros. O ataque obrigou grandes aeroportos europeus a recorrerem a operações manuais, causando atrasos generalizados e cancelamentos de voos. A perturbação foi mais grave nos aeroportos de Heathrow (Londres), Bruxelas, Brandeburgo (Berlim) e Dublin.

Nos termos da Diretiva SRI 2, um incidente é considerado "significativo" se, nomeadamente, causar graves perturbações operacionais dos serviços ou perdas financeiras à entidade em causa. Não obstante, nenhum Estado-Membro tratou este incidente como sendo significativo ou em grande escala com impacto transfronteiriço. Por conseguinte, nenhum dos Estados-Membros afetados o notificou formalmente à ENISA ou a outros Estados-Membros. A rede de CSIRT não aconselhou a UE-CyCLONe, que, por conseguinte, não apoiou a gestão coordenada do incidente.

Fonte: análise do TCE, com base em entrevistas a pessoal da ENISA.

- 39** Outra razão para a escassa comunicação de incidentes transfronteiriços é o facto de caber às autoridades de cada Estado-Membro determinar se um incidente notificado tem um impacto transfronteiriço e que outros Estados-Membros foram afetados. Segundo as informações de que dispõem, a entidade que notifica ou a autoridade do Estado-Membro pode não ter conhecimento da natureza transfronteiriça de alguns ataques. Atualmente, não existe uma plataforma à escala da UE que receba comunicações de incidentes em tempo real de todos os Estados-Membros e que possa conciliar informações sobre setores ou indicadores de comprometimento para detetar incidentes transfronteiriços. Por conseguinte, existe um risco elevado de que alguns incidentes deste tipo possam não ser sinalizados como tal e comunicados.
- 40** Nenhum incidente de cibersegurança é considerado "em grande escala" por nenhum Estado-Membro desde 2016. Em princípio, qualquer incidente que afete significativamente pelo menos dois Estados-Membros é abrangido por esta definição. Contudo, mesmo os incidentes de cibersegurança que causaram interrupções globais e danos avultados, como os apresentados na [figura 3](#), não foram considerados em grande escala. Consequentemente, o procedimento da UE-CyCLONe para a escalada da situação nunca foi plenamente ativado devido a um incidente de cibersegurança em grande escala.

Figura 3 | Exemplos de incidentes graves de cibersegurança



Fonte: TCE, adaptado de informações da [Cloudflare](#), da [ENISA](#), da [Europol](#), da [Wired](#), da [IBM](#) e da [CrowdStrike](#).

- 41** Além das obrigações de comunicação impostas às entidades e aos Estados-Membros, foi criada a rede de CSIRT para facilitar a partilha de informações. A confiança entre os Estados-Membros está no cerne desta rede, em que os dados são partilhados de forma voluntária. O valor acrescentado da rede reduz-se bastante se os Estados-Membros não estiverem dispostos a partilhar informações oportunas e práticas.
- 42** A partilha de informações ao nível da UE é restringida pela legislação de cada Estado-Membro em matéria de segurança. Se um país considerar que as informações relativas a um ciberataque a uma entidade de importância crítica são classificadas, ou que a comunicação de um incidente específico seria prejudicial para a segurança nacional, não é obrigado a partilhar os dados. Durante as visitas do Tribunal aos Estados-Membros, os representantes da rede de CSIRT e da UE-CyCLONe afirmaram que a partilha só pode ser feita dentro dos limites da legislação nacional em matéria de segurança. Não foi realizada ao nível da União uma análise dos quadros jurídicos dos Estados-Membros e do seu impacto na partilha de informações.

- 43** Em 2016, a rede de CSIRT era composta por 28 CSIRT nacionais, com dois representantes por Estado-Membro. A não partilha de informações tem sido um problema persistente. A [avaliação da Diretiva SRI pela Comissão](#) reconheceu que os Estados-Membros não partilham informações sistematicamente entre si, o que afeta em especial a eficácia das medidas de cibersegurança e o grau de conhecimento conjunto da situação ao nível da UE. Ao abrigo da Diretiva SRI 2, muitos Estados-Membros nomearam CSIRT nacionais e também setoriais, pelo que a rede se expandiu substancialmente. À data da auditoria, era composta por 42 CSIRT e mais de 700 participantes a título individual. Este panorama torna o reforço da confiança ainda mais desafiante, pois é difícil manter relações estreitas entre todos os membros.
- 44** A rede de CSIRT está ciente do problema de falta de partilha de informações e, à medida que se expande, está a ponderar várias ações para aumentar a confiança. A criação de polos mais pequenos de Estados-Membros que formem plataformas transfronteiriças, como descrito nos pontos [62](#) a [74](#), é uma estratégia alternativa a uma rede à escala da UE que pode ajudar a superar esta dificuldade.

Os serviços contratados pelo centro de situação cibernética duplicam parcialmente as capacidades existentes e não é claro como este centro funcionará no futuro

- 45** Nos termos da Diretiva SRI 2, nos casos em que um incidente de cibersegurança em grande escala, potencial ou em curso, tenha ou seja suscetível de ter um impacto significativo, a Comissão integra a UE-CyCLONe⁹. Este novo papel e a evolução do panorama das ameaças levaram a Comissão a criar, em 2022, um grupo de trabalho de coordenação no domínio da cibersegurança no âmbito da DG CNECT. Este grupo de trabalho inclui um centro de situação cibernética, que deverá ajudar a Comissão a aumentar o seu conhecimento da situação e visa apoiá-la nas suas responsabilidades institucionais na gestão de crises. Também deverá ajudar a DG CNECT a prestar aconselhamento a nível político.
- 46** Para criar o centro de situação cibernética, a Comissão recorre, em grande medida, a prestadores de serviços externos [contratados](#) em dezembro de 2022 por quatro anos e quase 18 milhões de euros. O Tribunal avaliou a criação do centro, as suas realizações e os planos da Comissão para o seu funcionamento futuro.

⁹ [Diretiva SRI 2](#), artigo 16º, nº 2.

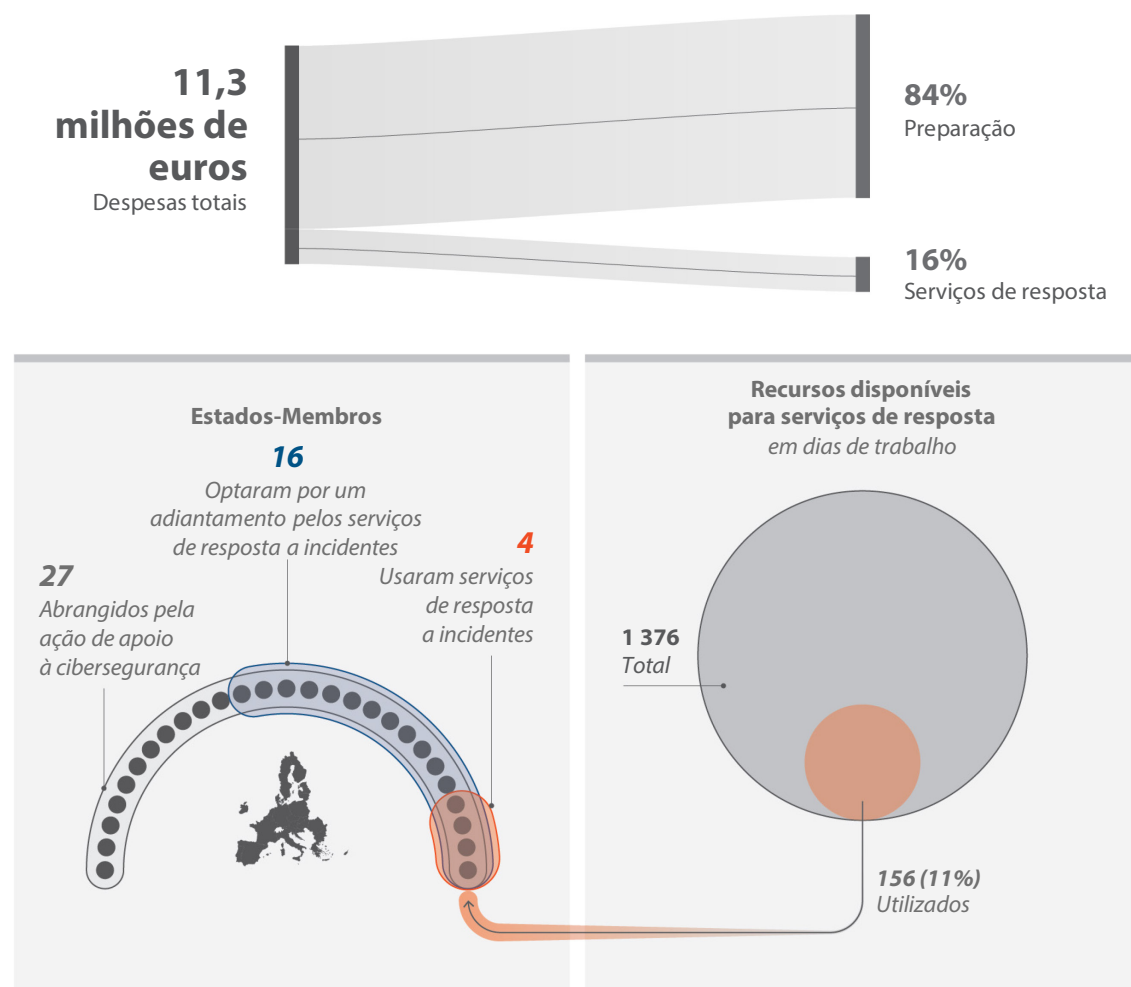
- 47** No âmbito dos serviços prestados, os contratantes criaram um painel baseado em fluxos comerciais de informações sobre ciberameaças, a fim de apresentar e partilhar informações sobre estas últimas. Elaboram igualmente vários relatórios de informações sobre ciberameaças, designadamente relatórios diários, semanais e temáticos sobre países ou setores económicos. O centro de situação cibernética físico (uma sala equipada com postos de trabalho ligados à distância ao painel alojado pelos contratantes) foi criado num dos edifícios da Comissão. À data da auditoria, era composto principalmente por um pequeno número de elementos do pessoal da Comissão, apoiados por muitos analistas dos contratantes e peritos da ENISA.
- 48** O Tribunal constatou que o trabalho realizado pelos prestadores de serviços externos para o centro de situação cibernética duplica parcialmente a capacidade existente da ENISA. Esta agência tem uma capacidade permanente de conhecimento da situação e de acompanhamento das ameaças. Publica regularmente relatórios sobre ciberameaças (por exemplo, relatórios sumários sobre incidentes específicos e relatórios semanais que apresentam uma panorâmica das ameaças), que se baseiam em informações de fonte aberta e são semelhantes aos elaborados pelos contratantes. Além disso, elabora ou contribui para sínteses de alto nível destinadas aos decisores políticos em tempos de crise, que também são comparáveis ao que o centro de situação cibernética produz.
- 49** Além disso, os dados utilizados pelo centro de situação cibernética para elaborar estes relatórios baseiam-se em fluxos comerciais de informações sobre ciberameaças e são semelhantes aos dados utilizados por outros serviços da Comissão, como a Direção-Geral dos Serviços Digitais e a CERT-UE. O Tribunal considera que a forma como este centro foi criado não tirou proveito suficiente do potencial de racionalização, não utilizando as informações que a Comissão e a ENISA já tinham disponíveis.
- 50** O contrato expira em dezembro de 2026, data após a qual os contratantes deixarão de prestar os serviços ao centro de situação cibernética. Estes serviços incluem o fornecimento dos dados disponíveis no painel e a elaboração dos relatórios de ameaças, além de constituírem a maioria do centro. O painel será entregue à Comissão, mas perderá o seu valor acrescentado se não for continuamente atualizado com informações sobre ciberameaças.
- 51** À data da auditoria, a Comissão não tinha planos acerca do apoio dado pelos prestadores de serviços externos para manter o centro de situação cibernética após o termo do contrato. O Tribunal considera que a ausência de um plano abrangente e pormenorizado para o futuro após o termo do contrato constitui um risco para o funcionamento deste centro após 2026.

A Reserva de Cibersegurança da UE permite a mobilização rápida de serviços de resposta a incidentes

- 52** Em 2022, na sequência imediata da agressão militar da Rússia contra a Ucrânia e reconhecendo que os ciberataques em grande escala se tinham tornado mais frequentes, a Comissão concedeu 15 milhões de euros em financiamento excecional à ENISA para testar a [ação de apoio à cibersegurança](#), lançada em 2023. Nesse ano, a Comissão concedeu financiamento adicional (cerca de 20 milhões de euros) para prolongar o programa até ao final de 2026.
- 53** A Comissão [propôs](#) igualmente o Regulamento de Cibersegurança (adotado em dezembro de 2024) como preparação para enfrentar incidentes de cibersegurança em grande escala. Este regulamento cria uma Reserva de Cibersegurança da UE, composta por serviços de resposta a incidentes de prestadores de confiança. Esta reserva começou a funcionar gradualmente em 2025, com um orçamento de 36 milhões de euros para o período entre 2025 e 2027.
- 54** O Tribunal avaliou a organização da ação de apoio à cibersegurança, dado que é a base da Reserva de Cibersegurança da UE. Também verificou se, ao conceber esta reserva, se aplicaram os ensinamentos retirados desde 2022.
- 55** A ENISA concebeu a ação de apoio à cibersegurança como mecanismo para prestar serviços de apoio à preparação dos Estados-Membros e à resposta destes a crises ou incidentes de cibersegurança em grande escala. Todos os serviços são pré-contratados pela ENISA, o que significa que os prestadores de serviços podem começar a trabalhar logo que os Estados-Membros o solicitem. Esta rapidez deve-se também à estrutura da ENISA, que garante que há um agente disponível a qualquer hora para tratar os pedidos dos Estados-Membros.
- 56** A ENISA optou por afetar o orçamento disponível equitativamente entre os Estados-Membros. Na prática, a Agência lançou um concurso aberto dividido em 27 lotes, um por Estado-Membro, com vista a selecionar um máximo de três prestadores privados de serviços de segurança para fornecerem serviços até ao final de 2026. Além disso, selecionou alguns prestadores de um lote pan-europeu para prestarem serviços a países terceiros elegíveis e a instituições, órgãos e organismos da UE, ou para apoiarem a resposta a incidentes transfronteiriços.

- 57** Este método permitiu à ENISA ter em conta os requisitos nacionais específicos, designadamente a língua, as credenciações de segurança nacionais ou a existência de uma presença estabelecida nos Estados-Membros. Por outro lado, como os prestadores não foram selecionados para poderem prestar serviços em toda a UE, este método tem a grande desvantagem de, se um Estado-Membro não utilizar os serviços pré-contratados, o orçamento autorizado para os serviços nesse país não poder ser utilizado para ajudar outro Estado-Membro.
- 58** Para a ação de apoio à cibersegurança, os Estados-Membros podiam escolher entre serviços de preparação, de resposta ou uma combinação de ambos. Optaram principalmente por utilizar o financiamento disponível para melhorar a preparação (84% das despesas em 2023). Os Estados-Membros que optaram por um adiantamento pelos serviços de resposta a incidentes (um acordo prévio com um prestador que garante que o Estado-Membro pode aceder aos serviços, mediante pedido, para dar uma resposta rápida a incidentes de cibersegurança) pouco o utilizaram, como mostra a [figura 4](#). Nos três Estados-Membros visitados, as autoridades manifestaram apreço pela gestão da ação de apoio à cibersegurança pela ENISA.

Figura 4 | Ação de apoio à cibersegurança da ENISA até 2023



Fonte: TCE, com base em dados da ENISA.

- 59** Entre 2024 e 2026, apenas nove Estados-Membros solicitaram a opção de adiantamento pelos serviços de resposta a incidentes. As entrevistas do Tribunal à ENISA e às autoridades de três Estados-Membros confirmaram uma forte preferência pelas atividades de preparação.
- 60** Embora a Reserva de Cibersegurança da UE vise principalmente apoiar a resposta e a recuperação no que diz respeito a incidentes graves de cibersegurança, os seus serviços que foram previamente afetados, mas não utilizados para a resposta a incidentes podem ser convertidos em serviços de preparação. Esta flexibilidade pode evitar que os serviços pré-pagos não sejam utilizados.
- 61** O Tribunal considera que o modelo escolhido para a Reserva de Cibersegurança da UE aplica os ensinamentos retirados da ação de apoio à cibersegurança. Porém, os dados sobre a utilização desta última apontam para o risco de a Reserva ser utilizada sobretudo para a preparação e não para a resposta, contrariamente à finalidade prevista no Regulamento de Cibersolidariedade.

O Sistema Europeu de Alerta em matéria de Cibersegurança visa melhorar as capacidades de deteção de ameaças, mas não está operacional

- 62** Um dos principais objetivos do Sistema Europeu de Alerta em matéria de Cibersegurança é incentivar a partilha de informações significativas para melhorar a deteção e análise de ciberameaças e a resposta às mesmas. A participação no sistema de alerta é voluntária, mas os Estados-Membros que optem por aderir a uma plataforma de cibersegurança transfronteiriça devem comprometer-se a partilhar as informações pertinentes com os outros membros. Trabalhando em conjunto em polos num ambiente seguro e de confiança, os Estados-Membros poderão evitar algumas das questões relativas à partilha de informações apontadas nos pontos [31](#) a [44](#).
- 63** À data da auditoria, 13 Estados-Membros tinham optado por integrar o Sistema Europeu de Alerta em matéria de Cibersegurança, criando duas plataformas transfronteiriças: a ATHENA e a ENSOC. Em 2026, foi atribuído financiamento para a criação de uma terceira (a NBCC), elevando a 20 o número de países que pertencem à rede (18 Estados-Membros, a Islândia e a Noruega¹⁰), como mostra a [figura 5](#).

¹⁰ Países terceiros associados nos termos do artigo 10º, nº 1, alínea a), do Regulamento (UE) 2021/694.

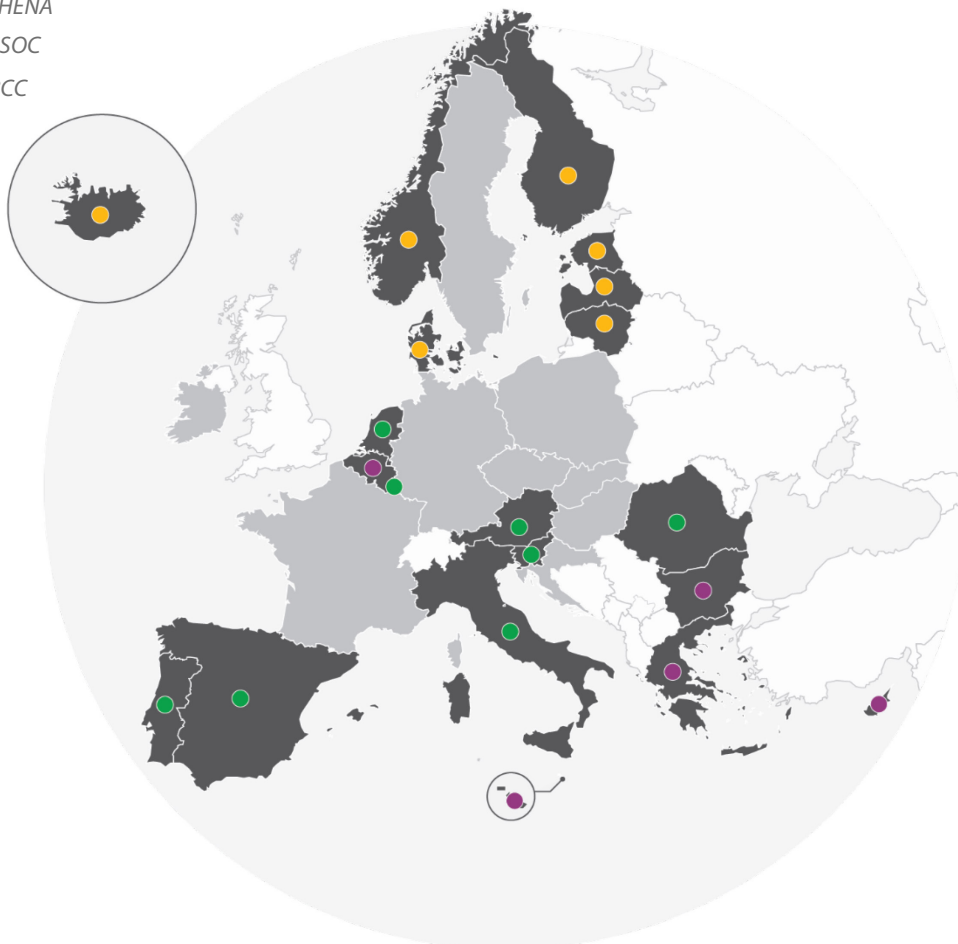
Figura 5 | Países que participam no Sistema Europeu de Alerta em matéria de Cibersegurança

■ Países que participam no Sistema Europeu de Alerta em matéria de Cibersegurança

● ATHENA

● ENSOC

● NBCC



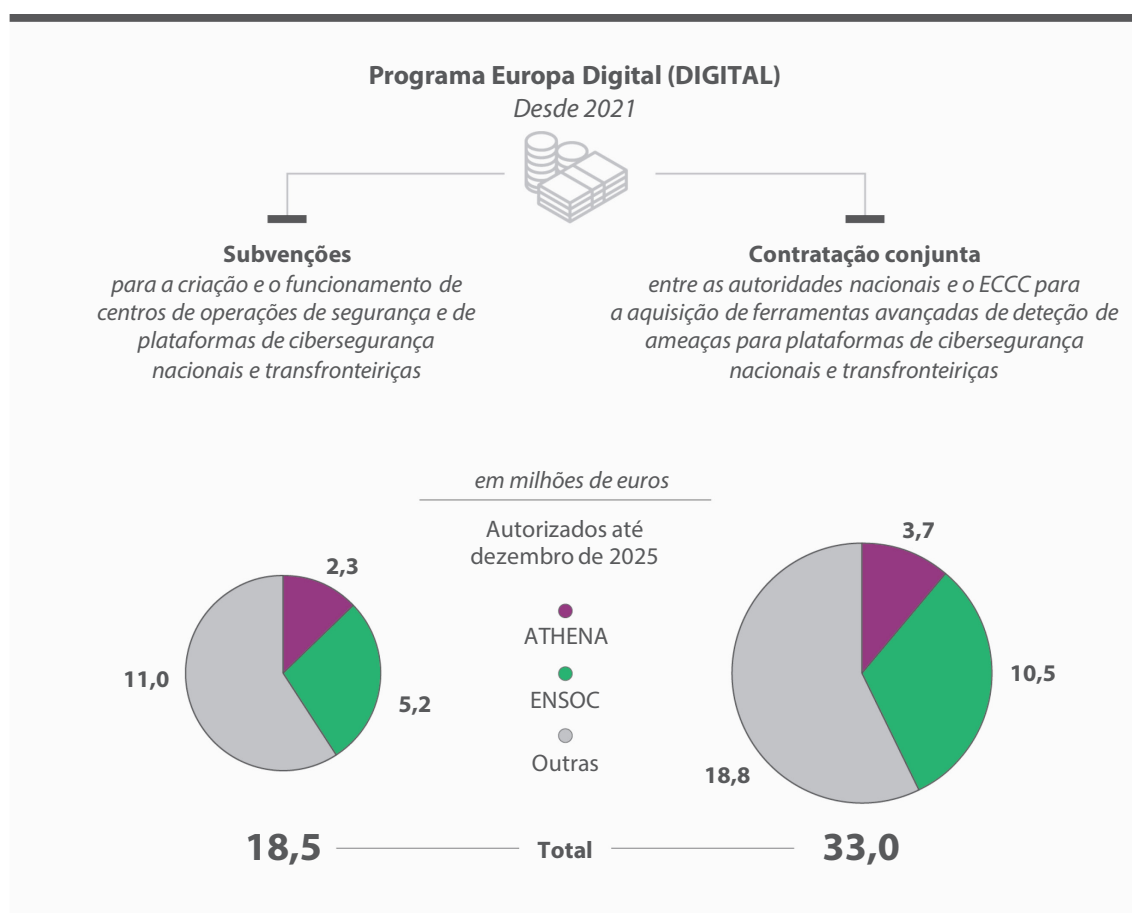
Fonte: TCE.

64 O Tribunal avaliou a forma como foram criadas as duas primeiras plataformas de cibersegurança transfronteiriças, bem como os progressos na concretização dos objetivos do Sistema Europeu de Alerta em matéria de Cibersegurança. Examinou também de que modo a criação de plataformas de cibersegurança transfronteiriças se enquadra no panorama mais vasto da cibersegurança e interage com as redes e estruturas existentes.

Não foram alcançados resultados concretos até à data devido a atrasos consideráveis na contratação

- 65** O financiamento de apoio à criação de plataformas de cibersegurança nacionais e transfronteiriças está disponível através do programa DIGITAL desde 2021. É concedido mediante um procedimento complexo com duas vertentes paralelas: subvenções tradicionais para apoiar a criação e o funcionamento das plataformas; e contratação conjunta para a aquisição de ferramentas avançadas de deteção de ameaças, como mostra a [figura 6](#). Após um convite à apresentação de propostas lançado em novembro de 2022, a ATHENA e a ENSOC iniciaram trabalhos em janeiro de 2024.

Figura 6 | Financiamento do Programa Europa Digital para plataformas de cibersegurança



Fonte: TCE, com base em dados da ECCC.

- 66** Foram organizados procedimentos de contratação limitados com duas fases¹¹ pelos membros da ATHENA e da ENSOC, bem como pela DG CNECT (primeira fase) e pelo recém-criado ECCC (segunda fase). O método com duas fases visa restringir a circulação de informações sensíveis, facultando as especificações técnicas pormenorizadas apenas aos candidatos selecionados na primeira fase.
- 67** A primeira fase foi lançada em maio de 2024 para a ENSOC e em julho de 2024 para a ATHENA. As empresas interessadas dispunham de um mês para se candidatarem. No entanto, os candidatos aprovados só foram notificados em abril de 2025, quase um ano após o lançamento do procedimento.
- 68** Além disso, nessa altura, não foi possível passar à segunda fase no procedimento de contratação da ENSOC nem no da ATHENA, pois os membros das plataformas e o ECCC não conseguiram transmitir às empresas pré-selecionadas as especificações técnicas necessárias para apresentarem uma proposta, dado que ainda as estavam a finalizar.
- 69** A segunda fase dos procedimentos de contratação só se iniciou em agosto de 2025 em relação a alguns lotes da ENSOC e estava prevista para o início de 2026 em relação à ATHENA. À data da auditoria, 18 meses após o lançamento do procedimento, não tinha sido celebrado nenhum contrato para qualquer dos lotes. O Tribunal considera que a falta de preparação adequada e a complexidade dos procedimentos de contratação prejudicaram a sua conclusão atempada.
- 70** Por conseguinte, o Tribunal constatou que as plataformas transfronteiriças não estão no bom caminho para alcançar os seus objetivos. Sem as ferramentas para detetar ameaças e partilhar informações, estão operacionalmente em suspenso. Acresce que o Sistema Europeu de Alerta em matéria de Cibersegurança ainda não está a funcionar, atrasando o desenvolvimento concreto de capacidades avançadas para detetar e prevenir ameaças e incidentes de cibersegurança. Foram assinadas alterações para prorrogar o prazo da convenção de subvenção, a fim de refletir os atrasos nos procedimentos de contratação até à data (15 meses para a ATHENA e 18 meses para a ENSOC).

¹¹ [Convite à apresentação de propostas da ENSOC](#) e [convite à apresentação de propostas da ATHENA](#).

As plataformas de cibersegurança transfronteiriças criam canais de comunicação adicionais que aumentam a complexidade

- 71** Uma das principais tarefas das plataformas de cibersegurança transfronteiriças consiste em partilhar informações pertinentes para melhorar a deteção de ameaças e a resposta às mesmas, designadamente sobre ciberameaças, vulnerabilidades, indicadores de comprometimento e autores de ameaças. As funções destas plataformas sobrepõem-se parcialmente às das CSIRT nacionais e às da rede de CSIRT, especialmente no que diz respeito à partilha de informações sobre ciberameaças e vulnerabilidades. Não existe uma fronteira clara entre as funções das plataformas e as das CSIRT. Segundo o Plano de Ação para a Cibersegurança de 2025 (ver ponto [29](#)), as plataformas de cibersegurança transfronteiriças devem funcionar tanto a nível técnico (como as CSIRT nacionais e a rede de CSIRT) como operacional (como a UE-CyCLONe).
- 72** O Regulamento de Cibersolidariedade exige que as plataformas de cibersegurança transfronteiriças celebrem acordos de cooperação entre si para facilitar a partilha de informações. A ENISA devia ter emitido orientações para a interoperabilidade entre estas plataformas até fevereiro de 2026, como exigido pelo referido regulamento. Entretanto, em dezembro de 2025, o ECCC concedeu uma subvenção a um consórcio (incluindo alguns membros da ENSOC e da ATHENA) para definir um quadro técnico de interoperabilidade entre plataformas de cibersegurança transfronteiriças. Contudo, as orientações e o quadro só serão concluídos quando as plataformas estiverem operacionais. Como o Tribunal salientou no seu parecer de 2023 sobre a proposta de Regulamento de Cibersolidariedade¹², existe o risco de, sem um acordo rápido, poderem ser desenvolvidos sistemas incompatíveis entre si, resultando num aumento dos custos.

¹² [Parecer 02/2023](#) sobre a proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança, ponto 26.

- 73** As plataformas de cibersegurança transfronteiriças são igualmente obrigadas a, sem demora injustificada, partilhar informações pertinentes sobre incidentes de cibersegurança em grande escala com a UE-CyCLONe e a rede de CSIRT. Ao nível dos Estados-Membros, a criação de plataformas de cibersegurança nacionais em simultâneo com a participação em plataformas transfronteiriças cria camadas adicionais de comunicação. A coordenação com os países terceiros que não são membros da rede de CSIRT¹³ ou da UE-CyCLONe também aumenta a complexidade.
- 74** São necessários acordos de cooperação claros para chegar a um consenso sobre uma taxonomia comum e a forma de partilhar informações e para assegurar a interoperabilidade. Os ensinamentos retirados da rede de CSIRT mostram que este é um desafio de monta. O Tribunal constatou que, à data da auditoria, não tinham sido acordados métodos de cooperação e partilha de informações. O Tribunal considera que a criação de plataformas de cibersegurança nacionais e transfronteiriças poderia promover uma partilha de informações mais eficaz. Porém, a integração das plataformas transfronteiriças no já complexo panorama de cibersegurança será difícil e exigirá canais de comunicação e métodos de cooperação adicionais.

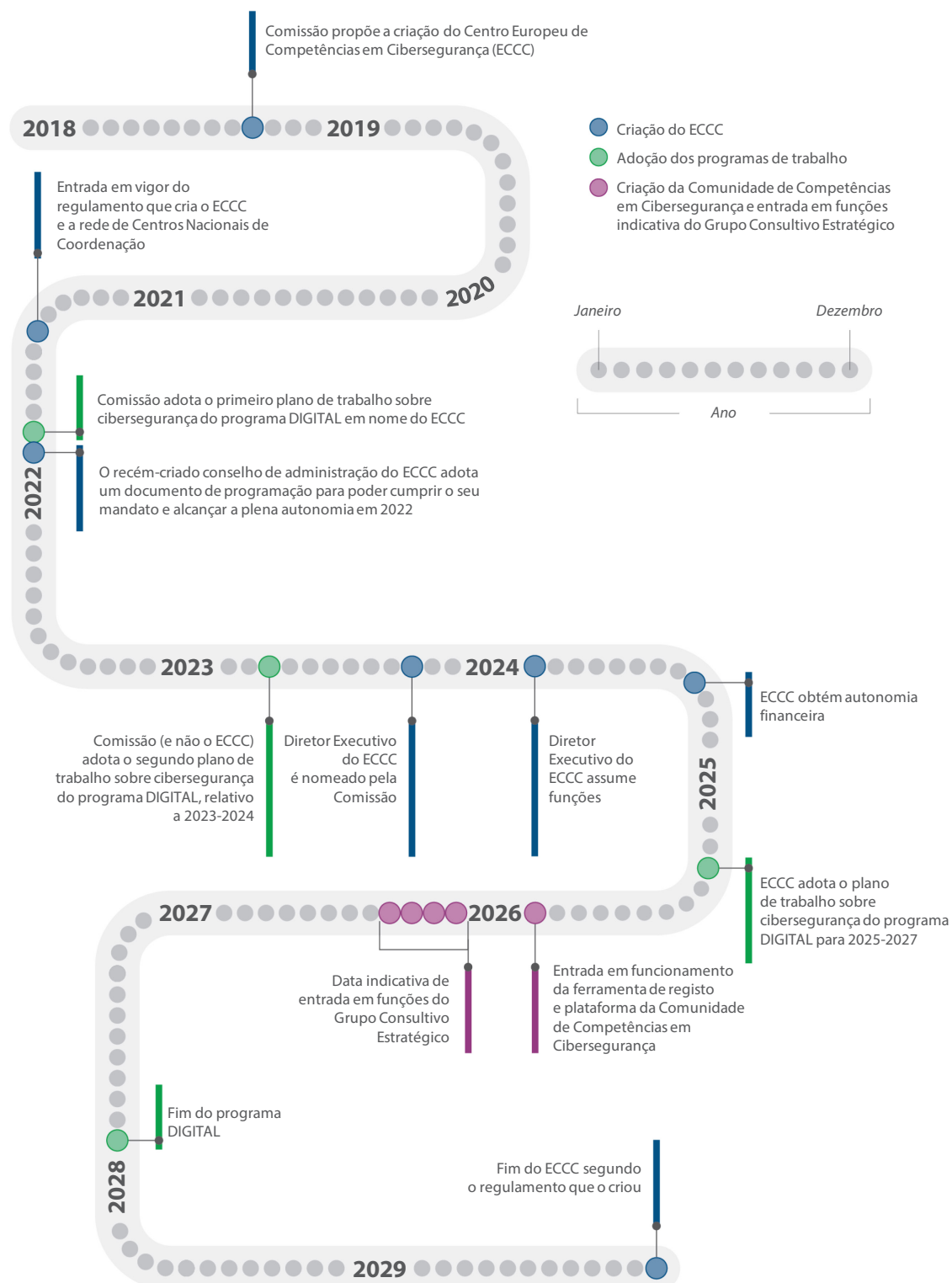
¹³ Islândia e Noruega.

Os projetos financiados pela UE no âmbito do programa DIGITAL visam reforçar a cibersegurança, mas enfrentam dificuldades na execução e na comunicação de informações

Os atrasos na criação da Comunidade de Competências em Cibersegurança impediram-na de adaptar o programa DIGITAL às suas necessidades

- 75** Para gerir a componente de cibersegurança do programa DIGITAL, em 2018 a Comissão propôs a criação do Centro Europeu de Competências em Cibersegurança (ECCC). O Regulamento ECCC previa que este Centro fosse apoiado por uma rede de 29 Centros Nacionais de Coordenação, um de cada Estado-Membro, mais a Islândia e a Noruega. Estipulou igualmente a criação da Comunidade de Competências em Cibersegurança (em seguida designada por "Comunidade"), composta por representantes da indústria, de organizações académicas e de investigação, bem como de outras associações pertinentes da sociedade civil.
- 76** Um máximo de 20 membros da Comunidade são nomeados para o Grupo Consultivo Estratégico, que é uma das três componentes da estrutura do ECCC. Uma das principais tarefas deste grupo é a organização de consultas públicas que contribuam para a agenda do ECCC e os planos de trabalho do programa DIGITAL.
- 77** O Tribunal avaliou se o programa DIGITAL e os seus planos de trabalho foram adotados após uma análise sólida das necessidades. Analisou também a forma como foi possível ao ECCC, à rede de Centros Nacionais de Coordenação, à Comunidade e ao Grupo Consultivo Estratégico contribuir para os referidos planos. Na prática, estas quatro entidades foram sendo criadas sucessivamente ao longo de vários anos (ver [figura 7](#)).

Figura 7 | Cronograma da criação do Centro Europeu de Competências em Cibersegurança, da rede de Centros Nacionais de Coordenação, da Comunidade e do Grupo Consultivo Estratégico



Fonte: TCE.

- 78** Uma vez que o ECCC só ficou plenamente operacional em setembro de 2024, a Comissão, em nome do Centro, adotou os programas de trabalho para 2021-2022 e 2023-2024. Nenhum deles pôde beneficiar do contributo da Comunidade.
- 79** Entretanto, os Estados-Membros começaram a criar os Centros Nacionais de Coordenação, que funcionam como pontos de contacto da Comunidade a nível nacional. A sua criação e funcionamento foram cofinanciados pelo programa DIGITAL. Até à data da auditoria, foram concedidos mais de 90 milhões de euros em financiamento da UE, incluindo cerca de 44 milhões de euros que serão distribuídos através de apoio financeiro a terceiros. Foi orçamentado um montante adicional de 38 milhões de euros até 2027 para apoio aos Centros Nacionais de Coordenação.
- 80** O Tribunal constatou que, em dezembro de 2025 (quatro anos após a criação do ECCC e da rede de Centros Nacionais de Coordenação), a Comunidade ainda não tinha sido criada e o Grupo Consultivo Estratégico ainda não tinha sido nomeado. O ECCC adotou o mais recente plano de trabalho sobre cibersegurança do programa DIGITAL em 14 de março de 2025, abrangendo o período entre 2025 e 2027. Embora o tenha elaborado e adotado após amplas consultas com os Estados-Membros e a rede de Centros Nacionais de Coordenação, não pôde beneficiar dos contributos e aconselhamento da Comunidade ou do Grupo Consultivo Estratégico. Esta situação contradiz as disposições do seu regulamento de base, e o Tribunal considera que se trata de uma oportunidade perdida.
- 81** O programa DIGITAL deverá terminar em 2027. Quanto ao ECCC, se o seu mandato não for prorrogado, deverá encerrar em 2029. Por conseguinte, o apoio da rede de Centros Nacionais de Coordenação, da Comunidade e do Grupo Consultivo Estratégico, quando estiverem em funcionamento, poderá ser relevante apenas durante um breve período.

Os projetos financiados pela UE visam objetivos pertinentes, mas muitos enfrentam problemas operacionais

82 O Tribunal extraiu uma amostra de 11 projetos pertinentes para a detecção de incidentes de cibersegurança e resposta aos mesmos, financiados ao abrigo do programa DIGITAL entre 2022 e 2025 (ver [figura 5](#) do [anexo I](#) e [anexo III](#)). Verificou se:

- os objetivos dos projetos estavam em consonância com os efeitos esperados indicados nos convites à apresentação de propostas e com os do programa DIGITAL em geral;
- até à data, os projetos alcançaram as realizações e os resultados previstos;
- as realizações dos projetos foram concretizadas dentro do prazo.

O produto desta avaliação é apresentado no [anexo IV](#).

Alguns projetos apresentam resultados iniciais, mas muitos enfrentam dificuldades operacionais e atrasos

83 O Tribunal constatou que todos os projetos têm finalidades que ajudam a alcançar os objetivos de cibersegurança do programa DIGITAL¹⁴ e que incidem na maioria dos objetivos dos convites à apresentação de propostas¹⁵.

84 Dos 11 projetos da amostra de auditoria, 2 estavam numa fase inicial de execução, pelo que não foi possível ao Tribunal chegar a uma conclusão sobre o seu desempenho. Dos restantes, o Tribunal considerou que quatro concretizaram de forma satisfatória as realizações e os resultados previstos. Entendeu que dois projetos apresentam algumas insuficiências e avaliou a concretização de três como insatisfatória (ver [anexo IV](#)).

85 O programa DIGITAL visa expressamente aumentar o nível de cibersegurança das pequenas e médias empresas (PME). A este respeito, vários projetos oferecem soluções concretas às PME (ver [caixa 2](#)).

¹⁴ Regulamento (UE) 2021/694 que cria o Programa Europa Digital, artigo 6º.

¹⁵ Convites *Capacity building of Security Operation Centres*, *Deploying The Network Of National Coordination Centres With Member States*, *Preparedness support and mutual assistance* e *Novel applications of AI and other enabling technologies for security operation centres*.

Caixa 2

Exemplos de projetos que produzem resultados concretos para as PME

O projeto [GR-SME-SOC](#) (projeto 6 no [anexo III](#)) visa proporcionar ferramentas e serviços de cibersegurança às PME na Grécia, criando um centro de operações de segurança adaptado às suas necessidades. Iniciou-se em janeiro de 2024 e está a ser executado por um consórcio de cinco organizações gregas. Prevê oferecer gratuitamente serviços de cibersegurança a 120 PME durante um ano, após o que os serviços ficarão comercialmente disponíveis. O projeto oferece às PME serviços avançados, como acompanhamento em tempo real, deteção de ameaças a partir de inteligência artificial (IA) e resposta ágil a incidentes.

Com o projeto [NCC-IE](#) (projeto 3 no [anexo III](#)), o seu coordenador disponibilizou cerca de 1,8 milhões de euros em subvenções a mais de 50 PME irlandesas para estas melhorarem a própria cibersegurança. O regime de subvenções beneficiou empresas que tinham entre 2 e cerca de 200 trabalhadores, incluindo empresas familiares, em fase de arranque e exportadoras mundiais em vários setores. As subvenções destinavam-se exclusivamente a empresas que tinham sido anteriormente sujeitas a uma análise de cibersegurança gerida pela agência pública Enterprise Ireland. Cobriam 80% dos custos (até um máximo de 60 000 euros) relativos à aplicação das recomendações da análise.

Fonte: TCE.

- 86** Muitos projetos da amostra do Tribunal estão a ter dificuldades no cumprimento dos prazos ou em termos operacionais (ver [anexo IV](#)). O Tribunal constatou que quatro projetos enfrentam atrasos consideráveis, designadamente a ENSOC e a ATHENA, como descrito nos pontos [65](#) a [70](#). A [caixa 3](#) apresenta mais exemplos.

Caixa 3

Exemplos de projetos que enfrentam atrasos e dificuldades operacionais

Na Irlanda, a Local Government Management Authority (LGMA) é a única beneficiária da subvenção ao projeto **ILG-SOC** (projeto 8 no [anexo III](#)). O objetivo do projeto é criar um centro de operações de segurança único para 31 autoridades locais, que poderão utilizar ferramentas avançadas de detecção de ameaças e resposta. O projeto teve início em outubro de 2023, com uma duração de três anos. A avaliação intercalar levou à rejeição de todas as prestações concretas. O projeto inclui vários procedimentos de contratação que foram mal-sucedidos ou sofreram atrasos. A duração do projeto será prolongada (sem qualquer financiamento adicional), o que poderá dar tempo suficiente para o concluir com sucesso.

Na Grécia, o projeto **EL-SOC** (projeto 5 no [anexo III](#)) visa criar um centro de operações de segurança consolidado a nível nacional, que reunirá informações dos centros setoriais. Esta consolidação proporcionará uma visão global abrangente e em tempo real da situação em matéria de cibersegurança. O projeto desenrola-se entre janeiro de 2024 e dezembro de 2026. A contratação prevista de *hardware* e serviços sofreu atrasos devido a problemas na finalização e publicação das especificações técnicas do convite à apresentação de propostas. Como razões para o atraso, o coordenador do projeto mencionou também questões relacionadas com a obtenção de cofinanciamento nacional e a reduzida disponibilidade do pessoal responsável pela contratação.

Fonte: TCE.

- 87** Dois outros projetos da amostra do Tribunal enfrentam atrasos moderados e três estão a produzir as realizações dentro do prazo. Por último, dois projetos encontram-se numa fase inicial de execução, pelo que não é possível ao Tribunal chegar a uma conclusão.

As restrições de segurança originaram dificuldades operacionais, e existem riscos significativos quando os controlos são realizados pelos beneficiários

- 88** O regulamento relativo ao programa DIGITAL prevê que, por razões de segurança, o financiamento da cibersegurança pode ser limitado a entidades estabelecidas na UE e controladas pelos Estados-Membros ou por cidadãos da União. Esta restrição visa atenuar o risco de intrusão ou influência por parte de Estados terceiros e impedir a partilha de informações de segurança sensíveis com autoridades de países terceiros.
- 89** A obrigação de a propriedade e o controlo estarem na UE aplica-se não só aos beneficiários de subvenções, mas também aos seus subcontratantes e a quaisquer beneficiários de apoio financeiro a terceiros. Com exceção desta última categoria (ver pontos [92](#) a [96](#)), a avaliação é realizada pelo serviço central de validação da [Agência de Execução Europeia da Investigação](#). No entanto, a decisão final sobre a elegibilidade para participar em convites restritos continua a caber à autoridade que concede a subvenção, ou seja, a DG CNECT ou o ECCC.
- 90** Durante o trabalho de auditoria, os beneficiários referiram repetidamente que as avaliações da propriedade e do controlo colocam dificuldades práticas. Avaliar se a propriedade e o controlo estão na UE pode ser um processo complexo e demorado. Exige uma análise de toda a estrutura de propriedade e da cadeia de controlo de cada organização, abrangendo todos os níveis de propriedade até aos proprietários finais. O serviço central de validação exige que cada entidade apresente amplas [provas documentais](#) da sua estrutura de propriedade e dos direitos específicos, governação da sociedade e quaisquer vínculos comerciais, financeiros ou de outra natureza que confirmem controlo.
- 91** Em três projetos financiados pela UE incluídos na amostra, pelo menos um beneficiário pertencente a um consórcio foi posteriormente excluído por se considerar que a sua propriedade ou controlo se encontravam fora da União. A exclusão de membros de um consórcio mostra que a noção de propriedade e controlo na UE não é plenamente compreendida por todos os participantes no programa DIGITAL. De modo geral, com base nos dados do serviço central de validação, entre 2022 e 2025, 7% de todos os candidatos ou subcontratantes no âmbito de subvenções deste programa para a cibersegurança foram reprovados na avaliação. A apresentação de candidaturas a um convite à apresentação de propostas por participantes inelegíveis causa atrasos, como exemplificado na [caixa 4](#).

Caixa 4

Exemplo de um caso de exclusão de beneficiários após reprovação nos controlos de segurança

Dois dos membros do consórcio do projeto **NG-SOC** (projeto 7 no [anexo III](#)) foram reprovados na avaliação da propriedade e do controlo. O resultado foi anunciado cerca de um mês antes do termo do prazo para a assinatura da convenção de subvenção. Dado que não havia tempo para encontrar um novo parceiro, o coordenador do projeto teve de aceitar assumir o trabalho que tinha sido atribuído aos dois membros excluídos. Um deles pertencia a um setor específico em que a solução desenvolvida iria ser testada, pelo que uma parte significativa do projeto, que dizia respeito ao ensaio das soluções na prática, não pôde avançar como previsto. A situação foi posteriormente corrigida mediante uma alteração da convenção de subvenção de modo a incluir novos membros.

Fonte: TCE.

- 92** Dois dos projetos examinados (NCC-IE e CYberSynchrony) prestam apoio financeiro a terceiros. Este mecanismo permite que os beneficiários de subvenções utilizem parte do montante recebido para financiar outras entidades através de concursos abertos. Este apoio pode facilitar o acesso ao financiamento da UE. Neste caso, os beneficiários são os únicos responsáveis pela realização das avaliações da propriedade e do controlo, sem participação do serviço central de validação.
- 93** Em 2021, a Comissão publicou orientações públicas gerais para os participantes em convites restritos, que atualizou em 2026. O apoio financeiro a terceiros está em vigor desde 2021 ao abrigo dos convites à apresentação de propostas do programa DIGITAL. Contudo, nem a Comissão nem o ECCC facultaram uma metodologia pormenorizada aos beneficiários sobre a forma de, ao avaliarem as entidades terceiras às quais prestam apoio financeiro, verificarem a propriedade e o controlo. Em julho de 2025, o ECCC partilhou orientações não vinculativas, proporcionando à rede de Centros Nacionais de Coordenação uma estrutura para as avaliações da propriedade e do controlo. O documento de orientação contém princípios gerais e medidas que é possível tomar. Porém, não especifica como realizar as verificações, deixando aos beneficiários a responsabilidade pelo desenvolvimento do seu próprio método.

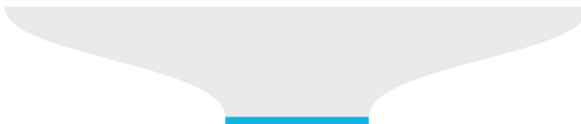
- 94** O Tribunal constatou que o ECCC não valida a metodologia adotada pelos beneficiários nem realiza controlos por amostragem para assegurar que a metodologia é suficientemente sólida e que a propriedade e o controlo dos destinatários selecionados para apoio financeiro se encontra realmente na UE.
- 95** No seu [Relatório Anual relativo a 2024](#), o Tribunal constatou que os beneficiários aos quais a Comissão confiou a gestão do apoio financeiro a terceiros (no domínio da investigação) não eram obrigados a demonstrar a eficácia dos controlos que realizavam para assegurar a regularidade das despesas da UE. Do mesmo modo, o ECCC não avalia a capacidade administrativa e técnica dos beneficiários para gerirem adequadamente as avaliações da propriedade e do controlo. Como descrito no ponto [90](#), estas avaliações podem ser complexas e são realizadas ao nível da UE por um serviço específico com conhecimentos especializados.
- 96** Neste contexto, o Tribunal considera que existe um risco considerável de os beneficiários, que são responsáveis por verificarem as avaliações da propriedade e do controlo, não terem capacidade para as realizar adequadamente. Dada a natureza das atividades financiadas, esta lacuna pode deixar expostos elementos sensíveis, como infraestruturas, dados operacionais e tecnologias de importância crítica para a segurança.

A maioria dos projetos financiados pela UE tem quadros de desempenho inadequados, e os dados do programa DIGITAL sobre o desempenho em termos de cibersegurança não são exatos

A maioria dos projetos financiados pela UE tem quadros de desempenho inadequados

- 97** Os beneficiários que gerem projetos financiados pela UE devem comunicar os progressos e resultados ao ECCC utilizando etapas intermédias, prestações concretas e indicadores, como ilustrado na [figura 8](#). O Tribunal avaliou se as etapas intermédias e prestações concretas definidas para cada projeto permitem o acompanhamento adequado dos mesmos. Analisou também se os indicadores de desempenho eram pertinentes e mensuráveis e se tinham uma base de referência e uma meta.

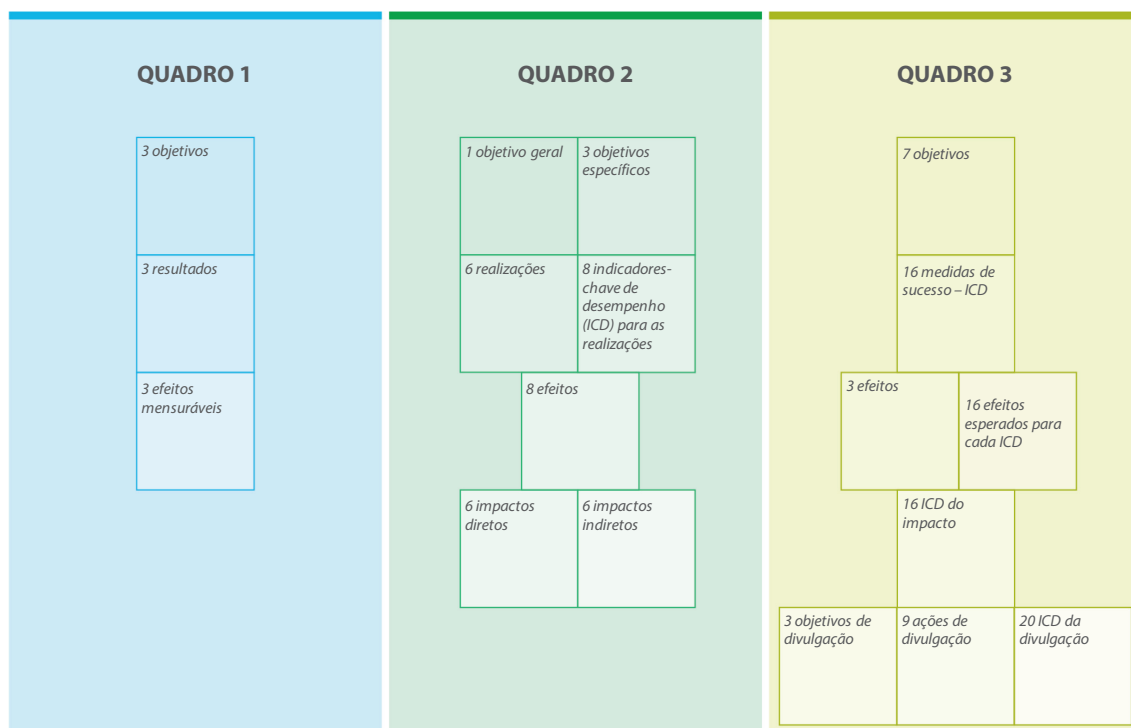
Figura 8 | Etapas intermédias, prestações concretas e indicadores de desempenho nos projetos do programa DIGITAL

	 Etapas intermédias	 Prestações concretas	 Indicadores de desempenho
O que são	Pontos de controlo ao longo do projeto que ajudam a registar os progressos	Realizações do projeto apresentadas para mostrar os progressos	Utilizados para medir os resultados
Forma de definição	Ligadas apenas às principais realizações (em número limitado)	Apenas as realizações principais (máximo de 10 a 15 por projeto)	Específicos, mensuráveis, atingíveis, relevantes e calendarizados
Exemplos	"Lançamento da fase-piloto da plataforma"	"Manual de utilização da plataforma"	"Redução de 30% do tempo de resposta a incidentes"
	 Abordagem estruturada, parte do sistema online para a gestão de subvenções		 Abordagem não estruturada

Fonte: TCE, com base no [formulário de candidatura a subvenções](#).

- 98** Na proposta de projeto, os beneficiários devem definir várias etapas intermédias e prestações concretas, seguindo a estrutura especificada nas instruções aos candidatos. Para facilitar o acompanhamento, todas as etapas intermédias e prestações concretas são enumeradas no sistema *online* para a gestão de subvenções. Normalmente, o ECCC analisa cada projeto duas vezes: a meio da execução e após a conclusão. Durante estas análises, os peritos externos verificam se as etapas intermédias e prestações concretas foram cumpridas e o ECCC valida essa avaliação. Por conseguinte, as etapas intermédias e prestações concretas são essenciais para o acompanhamento dos projetos e devem ser definidas de forma adequada.
- 99** O Tribunal constatou que quase nenhum dos projetos da amostra seguiu as instruções relativas ao número de etapas intermédias e prestações concretas: o número de etapas intermédias por projeto variava entre 8 e 39, e o número de prestações concretas entre 8 e 45. Muitas das etapas intermédias e prestações concretas não respeitam as instruções sobre a forma de elaboração, pelo que não são úteis para acompanhar os progressos (por exemplo, "reunião para iniciar a redação do convite à apresentação de propostas no âmbito da investigação" ou "atas das reuniões formais do projeto"). Em relação a três projetos, o comité de avaliação apontou estas questões antes da assinatura da subvenção. Em dois casos, os beneficiários apenas propuseram pequenas alterações (por exemplo, aos prazos) sem corrigir as questões fundamentais, ao passo que o terceiro não introduziu quaisquer alterações. Em relação a seis outros projetos da amostra, a análise do Tribunal mostra que as etapas intermédias ou prestações concretas não estão em conformidade com as instruções e nem sempre são adequadas. O Tribunal considera que a existência de prestações concretas ou etapas intermédias mal definidas ou em número excessivo dificulta o acompanhamento dos progressos.
- 100** Contrariamente às etapas intermédias e prestações concretas, os indicadores de desempenho não seguem uma abordagem estruturada e não estão consolidados num quadro do sistema de gestão de subvenções, encontrando-se em diferentes secções da proposta. Esta abordagem originou uma multiplicidade de quadros de desempenho propostos pelos beneficiários. Enquanto alguns apenas definiram objetivos de projeto associados a indicadores de desempenho, outros criaram quadros de desempenho muito mais complexos. A [figura 9](#) apresenta alguns exemplos.

Figura 9 | Exemplos da variedade de quadros de desempenho concebidos para os projetos



Fonte: TCE.

101 A análise do Tribunal conclui que muitos dos indicadores de desempenho utilizados pelos projetos não são pertinentes nem mensuráveis e não têm uma meta ou uma base de referência (ver [caixa 5](#)). Além disso, sete projetos definiram 20 ou mais indicadores, tendo um deles 52 indicadores. O produto desta avaliação é apresentado no [anexo IV](#).

Caixa 5

Exemplos de indicadores de desempenho inadequados

Não mensuráveis

- "Reforço das capacidades de cibersegurança das PME através de um indicador de comprometimento e de outros serviços prestados"
- "Disponibilização de ferramentas e métodos de resposta a incidentes que permitam a integração com os canais de comunicação da UE-CyCLONe"

Sem base de referência ou meta

- "Melhoria da preparação do pessoal $\geq 20\%$ "
- "Redução do esforço necessário para o alinhamento com as iniciativas pertinentes da UE em matéria de cibersegurança e o cumprimento das mesmas $\geq 20\%$ "

Sem relação com o desempenho

- "Relatório final sobre o projeto no fim da fase de financiamento"
- "Número de formandos que participarão em todas as sessões de formação"

Fonte: TCE, com base na documentação dos projetos.

102 De modo geral, o Tribunal considera que a grande variedade de quadros de desempenho, a má configuração dos indicadores e o seu número excessivo complicam significativamente o acompanhamento do desempenho. Por conseguinte, não é possível avaliar devidamente o desempenho dos projetos. Para complicar a situação, o modelo de relatório não contém uma secção específica sobre os indicadores de desempenho e, consequentemente, a maioria dos projetos da amostra do Tribunal não os apresentou.

Os dados sobre o desempenho da componente de cibersegurança do programa DIGITAL não são exatos

- 103** Para acompanhar as realizações do programa DIGITAL, o seu regulamento de base prevê indicadores de programa que todos os projetos devem comunicar, como descrito na [caixa 6](#).

Caixa 6

Indicadores do programa DIGITAL no domínio da cibersegurança

- 1.a O número de infraestruturas ou ferramentas de cibersegurança, ou ambas, adquiridas conjuntamente, incluindo no âmbito do Sistema Europeu de Alerta em matéria de Cibersegurança
- 1.b O número de infraestruturas ou ferramentas de cibersegurança, ou ambas, implantadas
- 2. O número de utilizadores e comunidades de utilizadores que obtêm acesso a instalações europeias de cibersegurança
- 3. O número de ações de apoio à preparação e resposta a incidentes de cibersegurança no âmbito do mecanismo de emergência em matéria de cibersegurança

Fonte: anexo II do [Regulamento \(UE\) 2021/694 que cria o Programa Europa Digital](#); quadro de acompanhamento e avaliação do Programa Europa Digital ([SWD\(2024\) 37](#)) [em inglês].

- 104** O Tribunal avaliou se os projetos incluídos na amostra comunicaram informações sobre estes indicadores e examinou a forma como o ECCC recolhe e verifica os dados conexos.
- 105** Todos os projetos devem comunicar informações sobre os indicadores do programa DIGITAL no sistema de gestão das subvenções antes das revisões intercalar e final. O Tribunal constatou que, dos sete projetos que estavam a meio do período de execução durante a auditoria e que, por conseguinte, deveriam ter comunicado informações sobre estes indicadores, apenas três o tinham feito. Destes, dois não transmitiram informações exatas: um facultou dados sobre o indicador errado e o outro apresentou os valores das metas em vez dos resultados alcançados.

106 Todos os anos, a Comissão comunica informações sobre estes indicadores nas suas [declarações de desempenho sobre o programa](#), que permitem às partes interessadas avaliar se este está a cumprir os seus objetivos. Segundo as declarações relativas a 2024, os indicadores do programa DIGITAL referentes à cibersegurança estão no bom caminho. O ECCC explicou ao Tribunal que, para compilar estes indicadores, recorreu a vários inquéritos enviados aos beneficiários dos projetos, em vez de os basear no sistema de gestão das subvenções. O Tribunal analisou os dados desagregados facultados pelo ECCC e detetou muitos problemas quanto à forma de recolha dos dados e à sua qualidade global. Constatou que os dados recolhidos não correspondem aos valores apresentados na declaração de desempenho sobre o programa, pelo que a forma de cálculo dos valores comunicados não é clara. Não encontrou provas de que a exatidão dos dados comunicados tenha sido verificada pelo ECCC. Com base nas verificações dos projetos constantes da amostra e dado que a maioria dos valores está em falta ou é inexata, o Tribunal considera que os dados comunicados não refletem adequadamente os resultados alcançados.

O presente relatório foi adotado pela Câmara III, presidida por George Marius Hyzler, Membro do Tribunal de Contas, no Luxemburgo, na sua reunião de 16 de junho de 2026.

Pelo Tribunal de Contas

Tony Murphy
Presidente

Anexos

Anexo I – Sobre a auditoria

- 01** A cibersegurança é definida como "as atividades necessárias para proteger de ciberameaças as redes e os sistemas de informação, os seus utilizadores e outras pessoas afetadas"¹. Uma ciberameaça é "uma circunstância, um evento ou uma ação potenciais suscetíveis de lesar, perturbar ou ter qualquer outro efeito negativo sobre as redes e os sistemas de informação, os seus utilizadores e outras pessoas"². A cibersegurança exige uma abordagem holística, que consiste numa série de atividades inter-relacionadas para prevenir e detetar ciberameaças, responder às mesmas e delas recuperar, como mostra a *figura 1*.

¹ Regulamento (UE) 2019/881 (Regulamento Cibersegurança).

² Regulamento Cibersegurança, artigo 2º.

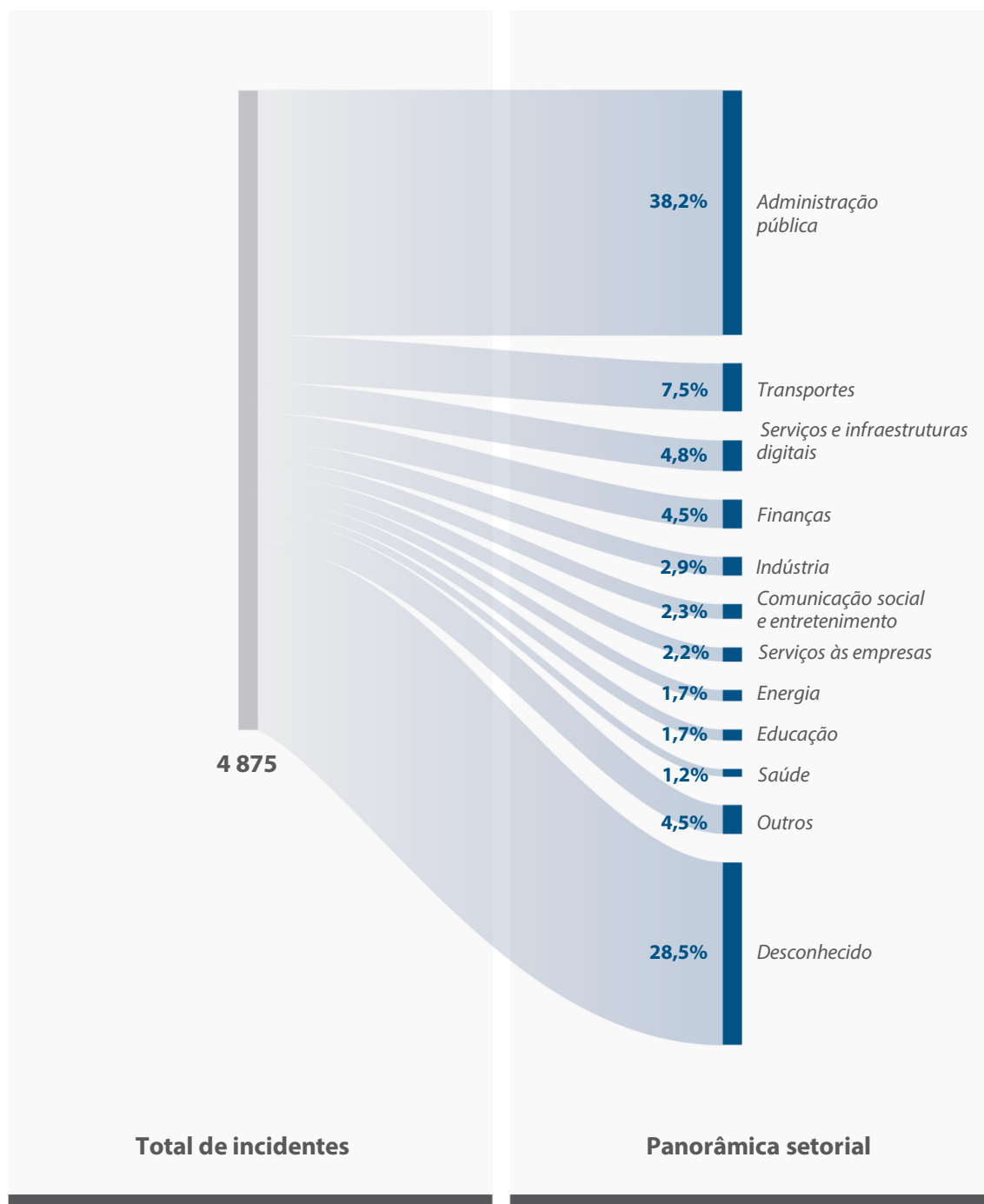
Figura 1 | Exemplos de atividades de cibersegurança

Prevenção 	Reduzir o risco de incidentes de cibersegurança e minimizar os seus efeitos potenciais <i>Exemplos: antivírus, barreiras de segurança (firewalls), encriptação, autenticação de dois fatores, gestão de atualizações de software, formação do pessoal sobre sensibilização para a segurança</i>
Deteção 	Descobrir atividades maliciosas <i>Exemplos: rastreamento das redes, conhecimento da situação</i>
Resposta 	Gestão e atenuação de um incidente de cibersegurança através da contenção da ameaça e da prevenção de novos danos <i>Exemplos: remoção de ameaças, contenção através do isolamento de servidores, desativação de contas expostas e redefinição de palavras-passe</i>
Recuperação 	Restabelecer a segurança e a operacionalidade dos sistemas, dados e serviços afetados <i>Exemplos: reinstalação de sistemas operativos nos servidores afetados, restauração dos dados das cópias de segurança, retirada de ensinamentos, atualização das políticas</i>

Fonte: TCE, com base no considerando 78 da Diretiva (UE) 2022/2555 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União (Diretiva SRI 2).

02 A [Agência da União Europeia para a Cibersegurança \(ENISA\)](#) considera que o nível de ameaças à cibersegurança é substancial, observando simultaneamente que o panorama neste domínio se tornou e continua a ser consideravelmente mais complexo³. Estas ameaças sublinham a importância vital da cibersegurança em economias e sociedades cada vez mais digitais. No seu [relatório do estado das ameaças em 2025](#), a ENISA identificou o *ransomware* como a ameaça mais grave na UE. A [figura 2](#) mostra os setores visados.

³ ENISA, [2024 Report on the State of Cybersecurity in the Union](#).

Figura 2 | Setores visados por ciberataques

Fonte: TCE, com base em dados da [ENISA](#).

Incidentes de cibersegurança significativos e em grande escala

03 Os incidentes de cibersegurança, que incluem ciberameaças e eventos não intencionais (como os mencionados no ponto [40](#) e na [figura 3](#) do corpo do relatório), "podem impedir a prestação de serviços públicos [e] o exercício das atividades económicas (...), gerar perdas financeiras importantes, minar a confiança dos utilizadores, causar graves prejuízos à economia e aos regimes democráticos da União e até ter consequências para a saúde ou ser potencialmente fatais"⁴. Um incidente de cibersegurança é considerado⁵:

- **significativo**, se tiver causado ou for suscetível de causar graves perturbações operacionais nos serviços ou perdas financeiras à entidade em causa, ou se tiver afetado ou for suscetível de afetar outras pessoas singulares ou coletivas, causando danos materiais ou imateriais consideráveis;
- **em grande escala**, se tiver causado um nível de perturbação superior à capacidade de resposta de um Estado-Membro ou que tenha um impacto significativo em, pelo menos, dois Estados-Membros.

04 Um incidente de cibersegurança em grande escala pode transformar-se numa verdadeira **crise de cibersegurança para a UE** se impedir o correto funcionamento do mercado interno ou colocar graves riscos em termos de segurança pública para entidades ou cidadãos em vários Estados-Membros ou na totalidade da União⁶.

⁴ Regulamento (UE) 2025/38 (Regulamento de Cibersolidariedade), considerando 2.

⁵ Diretiva SRI 2, artigos 6º e 23º, especificado de forma mais pormenorizada no Regulamento de Execução (UE) 2024/2690 da Comissão em relação a vários prestadores no setor das infraestruturas digitais.

⁶ Diretiva SRI 2, considerando 69.

Quadro político da UE

- 05** O ecossistema cibernético da UE é complexo, multifacetado e transversal a várias políticas internas, como a justiça e assuntos internos, o mercado único digital e a investigação⁷. Em matéria de política externa, a cibersegurança está patente na diplomacia e é uma parte cada vez maior da nascente política de defesa da União⁸.
- 06** Nos últimos anos, a UE reforçou o seu quadro regulamentar em matéria de cibersegurança. A *figura 3* abaixo apresenta os instrumentos legislativos e políticos mais pertinentes ao nível da UE. Em consonância com o âmbito da auditoria (ver pontos *13* a *14*), o Tribunal centrou-se nos instrumentos que lidam com a deteção de incidentes de cibersegurança significativos e em grande escala e com a resposta que lhes é dada.

⁷ Documento informativo do TCE, *Desafios à eficácia da política de cibersegurança da UE*.

⁸ Ver, por exemplo, *postura da União Europeia no ciberespaço* (2022), *enquadramento para uma resposta coordenada da UE às campanhas híbridas* (2022), *Política de Ciberdefesa da UE* (2023) e *Cyber Diplomacy Toolbox* (2023).

Figura 3 | Legislação e instrumentos políticos pertinentes da UE

- Adoção de legislação e instrumentos políticos
- Criação de redes e estruturas



Fonte: TCE.

Funções e responsabilidades

- 07** O panorama da cibersegurança na União Europeia envolve numerosas entidades públicas e privadas a nível regional, nacional e da UE (designadamente as autoridades policiais) na esfera civil. A cibersegurança é também um elemento fundamental da segurança e defesa nacionais⁹. O [anexo II](#) ilustra o panorama atual na União.
- 08** Os Estados-Membros da UE são os principais responsáveis pela prevenção de quaisquer incidentes e crises de cibersegurança que os afetem, pela preparação para os mesmos e pela resposta a dar-lhes. Nos termos do [artigo 4º, nº 2, do Tratado da União Europeia](#), a segurança nacional é da exclusiva responsabilidade de cada Estado-Membro. Dado que os incidentes de cibersegurança podem perturbar e danificar infraestruturas de informação de importância crítica das quais depende o bom funcionamento do mercado interno, a União também desempenha um papel importante em caso de incidente significativo ou crise¹⁰. A [figura 4](#) apresenta os principais intervenientes ao nível da UE.

⁹ Parecer 02/2023 sobre a proposta de Regulamento de Cibersolidariedade.

¹⁰ Plano de ação da UE para a gestão de cibercrises.

Figura 4 | Entidades ao nível da UE com papel importante na cibersegurança



Fonte: TCE.

Financiamento da UE

- 09** Ao abrigo do quadro financeiro plurianual para 2021-2027, a principal fonte de financiamento da cibersegurança é o [Programa Europa Digital](#) (DIGITAL). Lançado em 2021, é o primeiro programa da UE que visa especificamente impulsionar a transformação digital da União. Dispõe de um orçamento total de 8,1 mil milhões de euros¹¹.
- 10** O programa DIGITAL financia ações no domínio da cibersegurança no âmbito do seu objetivo específico nº 3, "Cibersegurança e confiança". Mais precisamente, existe um orçamento de 1,4 mil milhões de euros para:
- aumentar a coordenação em matéria de cibersegurança entre as ferramentas e infraestruturas de dados dos Estados-Membros;
 - apoiar uma implantação alargada das soluções em matéria de cibersegurança em todos os setores da economia.
- 11** A maioria do financiamento do programa DIGITAL para a cibersegurança é concedida através de convites à apresentação de propostas. Entre novembro de 2021 e dezembro de 2025, foram lançados 12 convites, para os quais estava disponível um total de 825 milhões de euros em financiamento da UE. Está previsto o lançamento de novos convites em 2026 e 2027, visando conceder mais 212 milhões de euros em subvenções.
- 12** Outro importante programa da União que apoia a cibersegurança é o [Horizonte Europa](#). Neste âmbito, os projetos de cibersegurança são financiados principalmente ao abrigo do [agregado 3](#), "Segurança Civil para a Sociedade", e em geral encontram-se numa fase incipiente em termos de maturidade devido à ênfase do Horizonte Europa na investigação e inovação. O [Mecanismo de Recuperação e Resiliência](#) também disponibiliza financiamento para medidas de cibersegurança.

¹¹ [Programa Europa Digital](#).

Âmbito e método da auditoria

13 O aumento das ciberameaças e o seu impacto potencial salientaram a necessidade de reforçar a ciber-resiliência coletiva. O Tribunal realizou a presente auditoria para avaliar se as ações da UE são eficazes a facilitar a deteção de incidentes de cibersegurança significativos e em grande escala e a resposta aos mesmos. Em especial, avaliou se foi esse o caso em relação:

- às redes e aos mecanismos ao nível da UE (nomeadamente, a rede de CSIRT, a UE-CyCLONE, o Sistema Europeu de Alerta em matéria de Cibersegurança, o centro de situação cibernética e a Reserva de Cibersegurança da UE);
- às ações financiadas pelo programa DIGITAL.

O Tribunal não abrangeu a cooperação policial ao nível da UE nem as ações de dissuasão no domínio da cibersegurança empreendidas a esse nível através de medidas diplomáticas ou atividades de defesa.

14 A auditoria abrange o período decorrido entre 2022 e 2025. Baseia-se numa análise dos documentos pertinentes, em visitas de auditoria a três Estados-Membros (Irlanda, Grécia e Itália) e em questionários escritos e entrevistas com partes interessadas pertinentes. A [figura 5](#) mostra a forma como o Tribunal obteve provas para sustentar as suas observações.

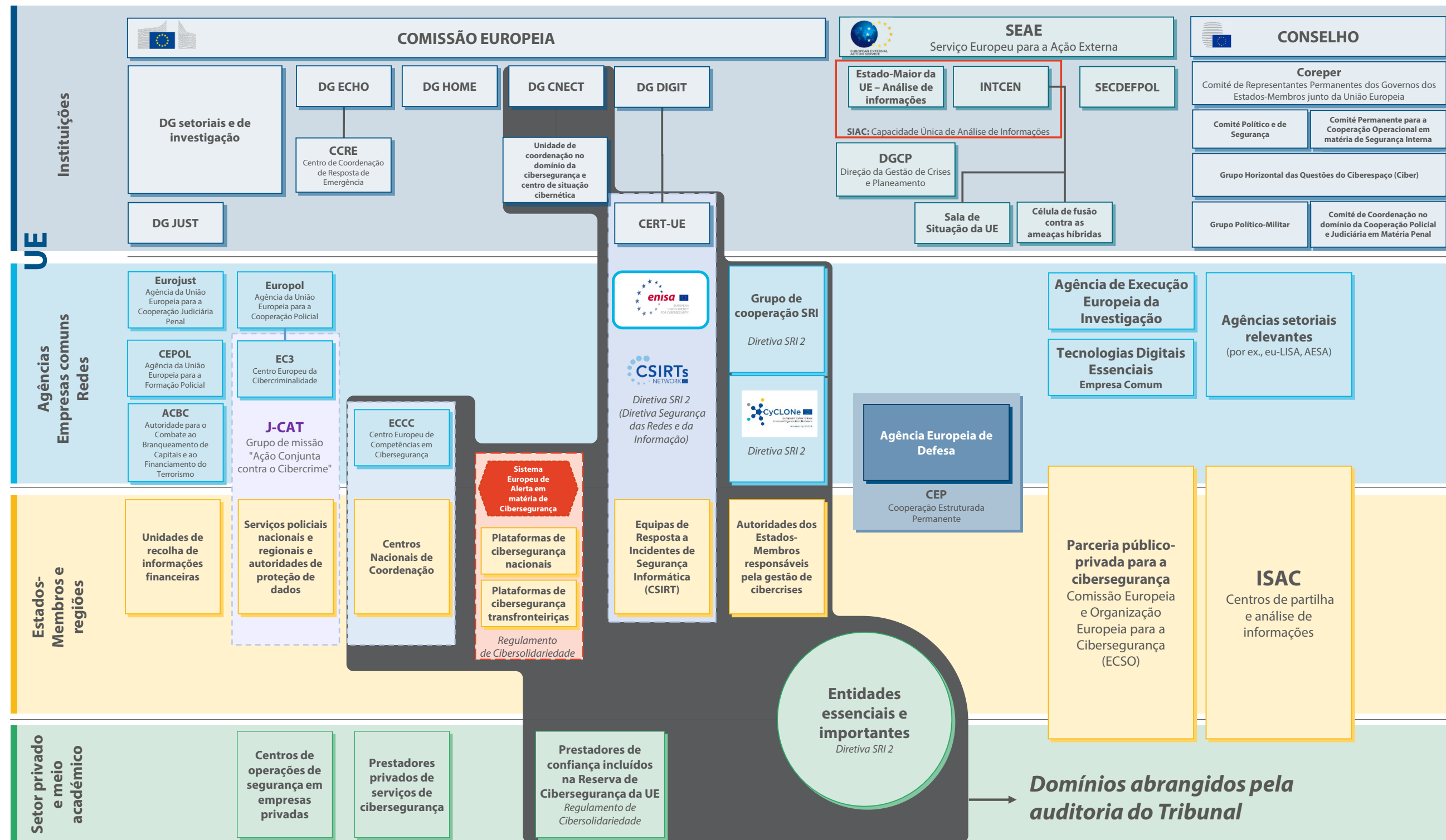
Figura 5 | Trabalhos de auditoria realizados

O Tribunal examinou	• O quadro jurídico aplicável à deteção de incidentes de cibersegurança significativos e em grande escala e à resposta aos mesmos • As funções e responsabilidades das redes e estruturas criadas ao nível da UE
O Tribunal analisou	• Documentos sobre o funcionamento da rede de CSIRT e da UE-CyCLONe • Documentação sobre a programação e o quadro de acompanhamento do desempenho do programa DIGITAL • Documentação sobre uma amostra de 13 ações financiadas pela UE (11 subvenções e 2 contratos – ver lista pormenorizada no anexo III) * O Tribunal selecionou ações financiadas pela UE em três países (Irlanda, Grécia e Itália) onde o financiamento pertinente do programa DIGITAL era mais avultado. As 11 subvenções foram extraídas de uma lista de 137 projetos financiados pela UE relevantes para a deteção de ameaças e resposta às mesmas, visando abranger uma combinação diversificada de projetos.
O Tribunal entrevistou	• Beneficiários das 11 subvenções financiadas pela UE incluídas na amostra • Representantes das autoridades nacionais de cibersegurança em três Estados-Membros (Irlanda, Grécia e Itália) • Representantes da Comissão Europeia (DG CNECT), da ENISA e do ECCC

Fonte: TCE.

- 15** As conclusões do Tribunal deverão contribuir para melhorar a eficácia e eficiência da capacidade de deteção e resposta da UE em relação a incidentes de cibersegurança significativos e em grande escala, bem como a seleção e o acompanhamento das ações financiadas pela União. A **metodologia de auditoria** do Tribunal está em conformidade com as normas internacionais de auditoria emitidas pela **Organização Internacional das Instituições Superiores de Controlo (INTOSAI)**.

Anexo II – Panorama de cibersegurança da UE



DG CNECT: Direção-Geral das Redes de Comunicação, Conteúdos e Tecnologias
DG ECHO: Direção-Geral da Proteção Civil e das Operações de Ajuda Humanitária Europeias
DG HOME: Direção-Geral da Migração e dos Assuntos Internos

DG JUST: Direção-Geral da Justiça e dos Consumidores
DG DIGIT: Direção-Geral dos Serviços Digitais
AESA: Agência da União Europeia para a Segurança da Aviação

UE-CyCLONE: Rede Europeia de Organizações de Coordenação de Cibersegurança
eu-LISA: Agência da União Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça

INTCEN: Centro de Situação e de Informações da UE
SECDEFPOL: Direção da Política de Segurança e Defesa

Anexo III – Ações de cibersegurança selecionadas

Nº	Título	Países	Data de início	Data de conclusão	Custo total (em milhões de euros) e contribuição da UE (em %)	Ligação para o portal "Funding & Tenders" da UE
Subvenções para plataformas de cibersegurança transfronteiriças que façam parte do Sistema Europeu de Alerta em matéria de Cibersegurança						
1	Establishing Cross-border SOCs (ATHENA)	Bulgária, Grécia, Chipre, Malta	1.1.2024	31.3.2028	4,7 (50%)	
2	ENSOC-CROSSBORDER PLATFORM (ENSOC)	Espanha, Itália, Luxemburgo, Países Baixos, Áustria, Portugal, Roménia	1.1.2024	30.6.2028	10,4 (50%)	
Subvenções para a implantação da rede de Centros Nacionais de Coordenação nos Estados-Membros						
3	Development and Implementation of the National Cyber Security Coordination and Development Centre for Ireland (NCC-IE)	Irlanda	2.10.2023	1.10.2026	4,2 (47%)	
4	Italian National Coordination Centre (NCC-IT)	Itália	1.11.2023	31.10.2025	2,0 (50%)	

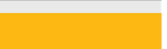
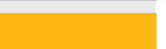
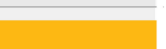
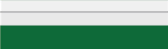
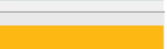
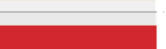
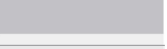
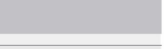
Nº	Título	Países	Data de início	Data de conclusão	Custo total (em milhões de euros) e contribuição da UE (em %)	Ligação para o portal "Funding & Tenders" da UE
Subvenções para reforçar a capacidade dos centros de operações de segurança, promover novas aplicações de IA e outras tecnologias facilitadoras para estes centros e prestar apoio à preparação e assistência mútua						
5	Enhancing the capacity of the Hellenic Consolidated Security Operation Center (EL-SOC)	Grécia, Chipre	1.1.2024	31.12.2026	9,7 (50%)	
6	Greek Security Operations Centre for Small and Medium Enterprises (GR-SME-SOC)	Grécia	1.1.2024	31.12.2026	12,1 (50%)	
7	Next Generation Security Operation Centres (NG-SOC)	Grécia, Espanha, Chipre, Luxemburgo, Eslovénia, Noruega	1.1.2024	31.12.2026	4,8 (50%)	
8	Irish Local Government Security Operations Centre (ILG-SOC)	Irlanda	1.10.2023	30.9.2026	8,3 (50%)	
9	An Interconnected Ecosystem of Cyber Security Coordination and Response Networks (Cyber-CORE-Network)	Irlanda	1.1.2024	31.12.2026	3,6 (50%)	
10	Harmonizing People, Processes, and Technology for Robust Cybersecurity (CYberSynchrony)	Bélgica, Grécia, Itália, Chipre, Países Baixos	1.6.2024	31.5.2027	7,0 (100%)	
11	Advanced Cooperative Security Operation Centres (ACSOC)	Grécia, Itália, Roménia	1.1.2025	31.12.2027	3,0 (50%)	

Nº	Título	Países	Data de início	Data de conclusão	Custo total (em milhões de euros) e contribuição da UE (em %)	Ligação para o portal "Funding & Tenders" da UE
Contrato-quadro para a ação de apoio à cibersegurança da ENISA						
12	Supporting ENISA for the Provision of Services under the Cybersecurity Support Action (28 lotes)	27 lotes para os Estados-Membros 1 lote pan-europeu	1.12.2022 ¹	31.12.2025	28,3 (100%)	
Contrato de prestação de serviços ao centro de situação cibernética da DG CNECT						
13	Bespoke Service to Support the Cyber Situation and Analysis Centre for the European Commission	-	30.12.2022	30.12.2026	18,0 (100%)	

Fonte: TCE.

¹ Múltiplos contratos celebrados ao longo de dezembro de 2022.

Anexo IV – Avaliação do Tribunal aos projetos de cibersegurança financiados pela UE

Nº Projeto		O projeto responde à maioria das necessidades indicadas no convite à apresentação de propostas	O projeto alcançou as realizações e os resultados previstos até à data	As realizações do projeto foram concretizadas no prazo previsto	Os indicadores de desempenho do projeto são pertinentes, mensuráveis e têm uma base de referência e uma meta
		 Satisfatória	 Algumas insuficiências	 Insatisfatória	 Não é possível tirar conclusões (demasiado cedo para concluir)
1	Establishing Cross-border SOCs (ATHENA)				
2	ENSOC-CROSSBORDER PLATFORM (ENSOC)				
3	Development and Implementation of the National Cyber Security Coordination and Development Centre for Ireland (NCC-IE)				
4	Italian National Coordination Centre (NCC-IT)				
5	Enhancing the capacity of the Hellenic Consolidated Security Operation Center (EL-SOC)				
6	Greek Security Operations Centre for Small and Medium Enterprises (GR-SME-SOC)				
7	Next Generation Security Operation Centres (NG-SOC)				
8	Irish Local Government Security Operations Centre (ILG-SOC)				
9	An Interconnected Ecosystem of Cyber Security Coordination and Response Networks (Cyber-CORE-Network)				
10	Harmonizing People, Processes, and Technology for Robust Cybersecurity (CYberSynchrony)				
11	Advanced Cooperative Security Operation Centres (ACSOC)				

Siglas, acrónimos e designações abreviadas

Sigla/acrónimo/designação abreviada	Definição/explicação
CSIRT	Equipa de Resposta a Incidentes de Segurança Informática
DG CNECT	Direção-Geral das Redes de Comunicação, Conteúdos e Tecnologias
DIGITAL	Programa Europa Digital
ECCC	Centro Europeu de Competências em Cibersegurança
ENISA	Agência da União Europeia para a Cibersegurança
PME	Pequena ou média empresa
SRI	Segurança das redes e da informação
UE-CyCLONe	Rede Europeia de Organizações de Coordenação de Cibercrises

Glossário

Termo	Definição/explicação
Autor de ameaças	Pessoa ou grupo que, intencionalmente, causa danos, perturba serviços ou rouba dados através da exploração de vulnerabilidades em sistemas, redes e dispositivos informáticos.
Centro de operações de segurança	Unidade organizativa que trabalha na prevenção de ameaças e incidentes de cibersegurança e recolhe informações conexas.
Ciberameaça	Possível utilização do ciberespaço para atacar a disponibilidade, autenticidade, integridade ou confidencialidade dos dados ou sistemas informáticos.
Incidente de cibersegurança	Evento que põe em perigo a disponibilidade, autenticidade, integridade ou confidencialidade dos dados ou sistemas informáticos.
Incidente de cibersegurança em grande escala	Incidente de cibersegurança que causa demasiadas perturbações para que um Estado-Membro consiga enfrentá-lo sozinho ou que tem um impacto significativo em pelo menos dois Estados-Membros.
Incidente de cibersegurança significativo	Incidente de cibersegurança que provocou ou pode provocar perturbações graves ou perdas financeiras a uma organização, ou danos consideráveis a outras entidades ou pessoas.
Plataforma de cibersegurança	Plataforma central que reúne vários serviços, ferramentas e profissionais de informática para melhorar o acompanhamento, a deteção e a análise de ciberameaças, prevenir incidentes de cibersegurança e apoiar a produção de informações neste domínio.
Ransomware (software de sequestro)	<i>Software</i> malicioso (<i>malware</i>) que nega à vítima o acesso a um sistema informático ou encripta os ficheiros, normalmente forçando-a a pagar um resgate para recuperar esse acesso.
Taxonomia	No contexto da cibersegurança, sistema de classificação utilizado para organizar, classificar e estruturar os conhecimentos sobre conceitos fundamentais, como ameaças e incidentes.

Respostas da Comissão

<https://www.eca.europa.eu/pt/publications/SR-2026-19>

Respostas do Centro Europeu de Competências em Cibersegurança (ECCC)

<https://www.eca.europa.eu/pt/publications/SR-2026-19>

Respostas da Agência da União Europeia para a Cibersegurança (ENISA)

<https://www.eca.europa.eu/pt/publications/SR-2026-19>

Cronologia

<https://www.eca.europa.eu/pt/publications/SR-2026-19>

Equipa de auditoria

Os relatórios especiais do TCE apresentam os resultados das suas auditorias às políticas e programas da UE ou a temas relacionados com a gestão de domínios orçamentais específicos. O TCE seleciona e concebe estas tarefas de auditoria de forma a obter o máximo impacto, tendo em consideração os riscos relativos ao desempenho ou à conformidade, o nível de receita ou de despesa envolvido, a evolução futura e o interesse político e público.

A presente auditoria de resultados foi realizada pela Câmara de Auditoria III – Ações externas, segurança e justiça, presidida pelo Membro do TCE George-Marius Hyzler. A auditoria foi efetuada sob a responsabilidade do Membro do TCE George-Marius Hyzler, com a colaboração de Romuald Kayibanda, chefe de gabinete, e Annette Farrugia, assessora de gabinete; Cyril Messein, responsável principal; Frédéric Soblet, responsável de tarefa; Jurgen Manjé e Flavia Di Marco, auditores. Zoe Amador Martínez prestou assistência linguística e Dunja Weibel deu apoio no domínio do *design* gráfico.



Da esquerda para a direita: Frédéric Soblet, Romuald Kayibanda, George-Marius Hyzler, Jurgen Manjé e Cyril Messein.

DIREITOS DE AUTOR

© União Europeia, 2026

A política de reutilização do Tribunal de Contas Europeu (TCE) encontra-se estabelecida na [Decisão nº 6-2019 do Tribunal de Contas Europeu](#) relativa à política de dados abertos e à reutilização de documentos.

Salvo indicação em contrário (por exemplo, em declarações de direitos de autor individuais), o conteúdo do TCE que é propriedade da UE está coberto pela licença [Creative Commons Attribution 4.0 International \(CC BY 4.0\)](#). Por conseguinte, regra geral, é autorizada a reutilização desde que sejam indicados os créditos adequados e as eventuais alterações. Esta reutilização do conteúdo do TCE não pode distorcer o significado ou a mensagem originais. O TCE não é responsável por quaisquer consequências da reutilização.

É necessário obter uma autorização adicional se um conteúdo específico representar pessoas singulares identificáveis, por exemplo, imagens do pessoal do TCE, ou incluir obras de terceiros.

Se for obtida uma autorização, esta anula e substitui a autorização geral acima referida e deve indicar claramente quaisquer restrições aplicáveis à sua utilização.

Para utilizar ou reproduzir conteúdos que não sejam propriedade da UE, pode ser necessário pedir autorização diretamente aos titulares dos direitos de autor.

Fotografia da capa: © 4AXY – stock.adobe.com.

Figuras 6 e 8 – ícones: concebidos com recursos de [Flaticon.com](#). © Freepik Company S.L. Todos os direitos reservados.

Figura 5 – mapas: [Eurostat](#).

O *software* ou os documentos abrangidos por direitos de propriedade industrial, nomeadamente patentes, marcas, desenhos e modelos registados, logótipos e nomes, estão excluídos da política de reutilização do TCE.

O conjunto de sítios Web institucionais da União Europeia, no domínio europa.eu, disponibiliza ligações a sítios de terceiros. Uma vez que o TCE não controla esses sítios, recomenda que se consultem as respetivas políticas em matéria de proteção da privacidade e direitos de autor.

Utilização do logótipo do TCE

O logótipo do TCE não pode ser utilizado sem o seu consentimento prévio.

HTML	ISBN 978-92-849-7887-8	ISSN 1977-5822	doi:10.2865/9760011	QJ-01-26-032-PT-Q
PDF	ISBN 978-92-849-7888-5	ISSN 1977-5822	doi:10.2865/6773074	QJ-01-26-032-PT-N

COMO CITAR ESTE DOCUMENTO

Tribunal de Contas Europeu, [Relatório Especial 19/2026](#), *Deteção e resposta a incidentes de cibersegurança – Quadro de cooperação da UE regista progressos, mas é apenas parcialmente eficaz devido a atrasos na execução e à escassa partilha de informações*, Serviço das Publicações da União Europeia, 2026

Nos últimos anos, a UE reforçou o seu quadro regulamentar em matéria de cibersegurança e criou redes e mecanismos para enfrentar incidentes de cibersegurança. Além disso, financia projetos neste domínio através do Programa Europa Digital.

O Tribunal conclui que as ações da União só em parte facilitam a deteção de incidentes de cibersegurança significativos e em grande escala e a resposta aos mesmos. Tem sido desenvolvido gradualmente um quadro de cooperação, mas os trabalhos para conseguir concluí-lo ainda estão em curso. A escassa partilha de dados, as insuficiências na comunicação de informações e os atrasos consideráveis na execução impedem as redes e os mecanismos da UE de atingirem todo o seu potencial. Os projetos visam objetivos pertinentes, mas muitos enfrentam problemas operacionais e atrasos. Acresce que existem insuficiências no quadro global de acompanhamento do desempenho. O Tribunal formula recomendações que visam corrigir estes aspetos.

Relatório Especial do TCE apresentado nos termos do artigo 287º, nº 4, segundo parágrafo, do TFUE.



TRIBUNAL
DE CONTAS
EUROPEU



Serviço das Publicações
da União Europeia

TRIBUNAL DE CONTAS EUROPEU
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tel. +352 4398-1

Informações: eca.europa.eu/pt/contact
Sítio Internet: eca.europa.eu
Redes sociais: @EUauditors