Respostas do Presidente do Comité Diretor da CERT-UE, da CERT-EU e da ENISA ao relatório especial do Tribunal de Contas Europeu sobre a segurança cibernética das instituições, órgãos e organismos da UE

1. Sumário Executivo

À luz do panorama de ameaças cibernéticas em constante evolução, a cibersegurança tornou-se crucial e da maior importância para as instituições, órgãos e organismos da UE que, cada vez mais, têm sido alvo de ciberataques altamente sofisticados nos últimos anos. No âmbito dos seus mandatos, a ENISA e a CERT-EU podem ambas prestar um apoio valioso às instituições, órgãos e organismos da UE, em matéria de cibersegurança e a diferentes níveis. A proposta da Comissão Europeia de um regulamento relativo a medidas para um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da UE constitui um instrumento fundamental neste contexto, um instrumento que a ENISA, a CERT-EU e o Presidente do Comité Diretor da CERT-EU apoiam veementemente.

Para o efeito, a ENISA, a CERT-EU e o Presidente do Comité Diretor da CERT-UE congratulam-se com o relatório especial do Tribunal de Contas Europeu sobre a segurança cibernética das instituições, órgãos e organismos da UE, publicado num momento manifestamente oportuno para endereçar o nível de preparação das instituições, órgãos e organismos da UE no seu conjunto. O relatório destaca claramente os papéis centrais que a ENISA e a CERT-EU podem desempenhar neste âmbito. O relatório define igualmente a necessidade de mais recursos e ações concretas especificamente orientadas para a melhoria da postura de segurança cibernética das instituições, órgãos e organismos da UE.

Com este entendimento, a ENISA, a CERT-EU e o Presidente do Comité Diretor da CERT-UE apoiam as principais observações e recomendações do relatório, que estão igualmente alinhadas com as propostas legislativas da Comissão Europeia nos domínios da segurança cibernética e da segurança da informação para as instituições, órgãos e organismos da UE.

As observações na secção seguinte destinam-se a fornecer esclarecimentos adicionais a certas áreas do relatório, em especial no que se refere ao trabalho relevante já realizado pela ENISA e/ou pela CERT-EU, bem como às ações previstas pela ENISA e/ou pela CERT-EU, especialmente nas áreas do reforço das capacidades das instituições, órgãos e organismos da

UE. No que diz respeito às recomendações, a ENISA e a CERT-EU aceitam a Recomendação 3 (Aumentar o foco da CERT-EU e da ENISA nas instituições, órgãos e organismos da UE menos maduros), especificamente dirigida a estas duas entidades.

2. Observações principais

A ENISA e a CERT-UE apoiam as principais observações formuladas pelo Tribunal de Contas. Dito isto, são apresentados seguidamente alguns esclarecimentos adicionais, especialmente no que se refere às ações empreendidas pela ENISA e/ou pela CERT-EU, bem como aos planos já estabelecidos para atividades futuras.

Ponto 49.

No que se refere ao pedido formal enviado pelo ICTAC ao Presidente do Comité Diretor da CERT-UE relativo ao direito de voto no comité, gostaríamos de esclarecer o seguinte:

Tendo em conta as despesas gerais consideráveis que a revisão do atual AII teria implicado, e porque os trabalhos em curso sobre o «Regulamento relativo a medidas para um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União» já tinham abordado a representação das agências descentralizadas, foi acordado resolver formalmente a questão, numa perspetiva de longo prazo, através do regulamento. Até lá, tal como confirmado pelo Presidente, manter-se-ão as práticas atuais e os pontos de vista expressos pelos representantes do ICTAC serão sempre bem-vindos e tidos em conta, tanto quanto possível e dentro da devida razoabilidade.

Ponto 66.

No final de 2021, a ENISA estabeleceu um plano de ação para ciber-exercícios, que inclui especificamente as instituições, órgãos e organismos da UE. No primeiro trimestre de 2022, será apresentado um plano de ação relevante para formação dirigida às instituições, órgãos e organismos da UE.

Caixa 3

Embora tal não seja explicitamente mencionado como outputs operacionais, a ENISA tem vindo a prestar apoio operacional e a cooperar com várias instituições, órgãos e organismos da UE, com base nos seus pedidos. Por exemplo, em 2018, no âmbito do “Objetivo 2.2. Apoio

na execução das políticas da União Europeia":

- O Banco Central Europeu solicitou apoio para o desenvolvimento do quadro de testes da *red team* do Eurosistema.
- A Agência Europeia para a Segurança da Aviação (EASA) solicitou apoio para o desenvolvimento dos objetivos do Centro Europeu para a Cibersegurança na Aviação, com vista à sensibilização para a cibersegurança e para a aplicação setorial da Diretiva relativa à segurança das redes e da informação.
- A Agência Ferroviária Europeia solicitou apoio na implementação da Diretiva relativa à segurança das redes e da informação no setor ferroviário, em especial apoio para o desenvolvimento de um centro setorial de partilha e análise de informação (ISAC) destinado a gestores de infraestruturas e empresas ferroviárias, bem como no âmbito do reforço das capacidades (organização de sessões de formação e sensibilização).
- A ENISA apoiou a Agência da União Europeia para a Gestão Operacional de Sistemas informáticos de grande escala nas áreasda liberdade, segurança e justiça (EU-LISA) nos seus esforços de melhoria da sua proficiência no domínio da cibersegurança e da continuidade do negócio/operações. Em especial, a ENISA ofereceu a sua experiência na organização dos exercícios e no desenvolvimento de cenários, tendo igualmente disponibilizado o plenamente desenvolvido CEP da ENISA à EU-LISA, a fim de organizar um exercício de preparação para um dos sistemas informáticos vitais da União Europeia.

Para além disso, desde 2019, a ENISA tem vindo a colaborar ativamente com as instituições, órgãos e organismos da UE (por exemplo, ERA, EMSA, AESA, ACER), no apoio à Diretiva relativa à segurança das redes e da informação, em atividades setoriais de formação de conhecimentos e sensibilização para a cibersegurança, bem como em iniciativas setoriais de política de cibersegurança conexas.

Ponto 71.

A ENISA desenvolveu em 2021 e lançará em 2022 uma formação especializada sobre «Como criar um programa de sensibilização e utilizar exercícios teóricos de simulação», tendo como destinatários específicos as instituições, órgãos e organismos da UE. No contexto da sua

cooperação estruturada, a ENISA e a CERT-EU também disponibilizarão formação conjunta às instituições, órgãos e organismos da UE em 2022.

Ponto 72.

Importa salientar que os exercícios de cibersegurança da ENISA têm um vasto âmbito e um vasto público, incluindo também as instituições, órgãos e organismos da UE. Esta abordagem permite igualmente responder às diversas necessidades das instituições, órgãos e organismos da UE, uma vez que estas podem beneficiar significativamente desses exercícios com os representantes dos Estados-Membros. É de salientar o facto de a ENISA ter vindo a envolver, desde 2016, o pessoal técnico das instituições, órgãos e organismos da UE como participantes nos exercícios europeus de cibersegurança, sob a orientação da CERT-EU, que é a entidade responsável pelo planeamentodesta ação. No seguimento destes esforços, a ENISA planeia, na sua estratégia de exercícios de 2022 e no âmbito das atividades de reforço de capacidades, promover um novo produto que será fornecido com o apoio da CERT-EU, com vista a oferecer às instituições, órgãos e organismos da UE oportunidades de formação em matéria de exercícios de autoavaliação.

3. Conclusões e recomendações

A ENISA e a CERT-EU aceitam a Recomendação 3 (Aumentar a atenção da CERT-EU e da ENISA às instituições, aos órgãos e aos organismos da UE menos maduros), especificamente dirigida a estas duas entidades.