RESPOSTAS DA COMISSÃO EUROPEIA

AO RELATÓRIO ESPECIAL DO TRIBUNAL DE CONTAS EUROPEU:

Cibersegurança nas instituições, organismos e agências da UE: o nível de preparação não é proporcional às ameaças

Conteúdo

O presente documento apresenta as respostas da Comissão Europeia às observações de um relatório especial do Tribunal de Contas Europeu, em conformidade com o artigo 259.º do Regulamento Financeiro, a publicar juntamente com o relatório especial.

I. RESPOSTAS SUCINTAS DA COMISSÃO

a) Introdução geral

A cibersegurança tornou-se uma das principais prioridades políticas e operacionais da Comissão Europeia. A crise da COVID-19 acelerou a nossa dependência dos serviços digitais (computação em nuvem, dispositivos móveis, inteligência artificial). Nos últimos dois anos, assistimos a uma transição em massa para o trabalho a partir de casa. Isto significa que tanto a cibercriminalidade como a ciberespionagem, as duas principais ameaças com que se confrontam as instituições, organismos e agências da União Europeia, também estiveram efetivamente em linha. A Comissão reconhece esta tendência e exibiu uma liderança coerente e determinada em matéria de cibersegurança. O Regulamento Cibersegurança entrou em vigor em 2019, nomeadamente alargando o mandato da ENISA e dando-lhe uma caráter permanente. Este regulamento estabeleceu igualmente uma cooperação formal entre a ENISA e a CERT-UE (a equipa de resposta a emergências informáticas que apoia todas as instituições, organismos e agências da UE). Em 2020, a Comissão propôs um reforço da Diretiva Segurança das Redes e da Informação, que está prestes a ser aprovada pelos legisladores.

A Estratégia para a Cibersegurança de 2020 continha igualmente três ações relacionadas com a cibersegurança das instituições, organismos e agências da UE. A Comissão anunciou a elaboração de um regulamento relativo à segurança da informação nos organismos e agências das instituições da UE e de um regulamento relativo às regras comuns em matéria de cibersegurança para as instituições, organismos e agências da UE, bem como a sua intenção de criar uma nova base jurídica para reforçar o mandato e o financiamento da CERT-UE, de forma a assegurar que dispõe dos recursos adequados face ao aumento das ameaças, dos riscos e dos incidentes.

Os trabalhos de preparação destas propostas avançaram. Embora ainda não tenham sido adotadas pelo Colégio, espera-se que o sejam no primeiro trimestre de 2022. As questões importantes debatidas entre as instituições nesta fase preparatória dizem respeito à base jurídica da proposta, bem como à capacidade orçamental de todas as instituições, organismos e agências da UE para satisfazer os requisitos em termos de financiamento das suas próprias necessidades de cibersegurança e para encontrar os recursos necessários para apoiar a CERT-UE em termos de orçamento e, em especial, de pessoal.

O nível de preparação para a cibersegurança das instituições, organismos e agências da UE tem diferentes níveis de maturidade. Várias instituições, organismos e agências da UE têm um forte desempenho em termos de ciberpreparação e devem continuar a servir de líderes, estimulando e inspirando progressos e novas melhorias em todo o panorama da cibersegurança. A fim de alcançar progressos mensuráveis, é importante reconhecer os diferentes níveis de maturidade entre as instituições, organismos e agências da UE e definir prioridades, orientando as ações de melhoria prioritariamente para as que apresentam lacunas que implicam uma maior exposição ao risco.

b) Posição da Comissão sobre as principais observações e recomendações do TCE

A Comissão congratula-se com o relatório do TCE sobre a cibersegurança das instituições, organismos e agências da UE. Regista que o relatório sublinha a importância de quadros jurídicos

comuns em matéria de segurança da informação e cibersegurança para todas as instituições, organismos e agências da UE, a fim de aumentar o nível global de cibersegurança em todos os domínios. A Comissão observa que as principais observações e recomendações do TCE não visam a cibersegurança operacional da própria Comissão, mas sim o papel político da Comissão de propor legislação para aumentar a maturidade cibernética das instituições, organismos e agências da UE.

Os futuros regulamentos relativos à «segurança da informação nos organismos e agências das instituições da UE» e às «regras comuns de cibersegurança para as instituições, organismos e agências da UE» definirão regras comuns para alcançar elevados níveis de segurança da informação e cibersegurança, mas a sua aplicação, no contexto organizacional e operacional das diferentes instituições, organismos e agências da UE (em especial, os seus perfis de ameaça e de risco), continua a ser da sua responsabilidade autónoma. A proposta de regulamento relativo à cibersegurança disporá de mecanismos de conformidade adequados e proporcionais ao objetivo e ao âmbito de aplicação das novas regras, sem prejuízo da autonomia das instituições, órgãos e agências.

A Comissão preside atualmente ao subgrupo «cibersegurança» do Comité Interinstitucional para a Transformação Digital (ICDT), que é uma função rotativa (por um período máximo de dois anos). Note-se que não foram atribuídos recursos específicos ao trabalho do subgrupo: todas as ações assentam nos melhores esforços envidados pelos participantes numa base voluntária.

A Comissão concorda com a ideia geral de reforçar os recursos e o mandato da CERT-UE, apoiando as principais observações e recomendações do relatório. A nossa posição pormenorizada é explicada nas observações adicionais da parte III. No que diz respeito às recomendações, a Comissão aceita as recomendações 1, alíneas a), b), c), d), e), f) e g), e 2, alíneas a), b) e c).

c) Últimos desenvolvimentos e próximas etapas

Foi concluída uma consulta formal a nível dos diretores-gerais das instituições, organismos e agências da UE sobre os projetos consolidados dos dois regulamentos (segurança da informação e cibersegurança), estando em curso a avaliação das respostas recebidas, antes da conclusão do pacote e da adoção pelo Colégio no primeiro trimestre de 2022.

II. RESPOSTAS DA COMISSÃO ÀS PRINCIPAIS OBSERVAÇÕES DO TCE

1. Níveis de maturidade em matéria de cibersegurança das instituições, organismos e agências da UE

A Comissão concorda que, ao analisar o nível de despesas das instituições, organismos e agências da UE em matéria de cibersegurança, é importante ter em conta as ameaças e os riscos.

Do mesmo modo, no que diz respeito aos recursos humanos, a estabilidade do pessoal das instituições, organismos e agências da UE é influenciada por uma série de fatores. O mercado de recrutamento de peritos especializados em cibersegurança é cada vez mais complexo. Em muitos casos, as regras em matéria de recursos humanos não estão adaptadas a perfis especializados (recrutamento, progressão na carreira, formação). Além disso, a pressão generalizada exercida pela

autoridade orçamental sobre os níveis de pessoal das instituições, organismos e agências da UE significa que domínios emergentes de elevada prioridade, como a cibersegurança, continuam a dispor de postos insuficientes, nomeadamente nos serviços operacionais internos.

A referência aos progressos em matéria de governação e gestão dos riscos deve ter em conta o facto de o controlo da conformidade estar agora a passar da fase piloto para a plena implantação. Assim, é normal que a cobertura seja até agora bastante baixa. Este projeto de conformidade é a próxima fase de um processo de melhoria da maturidade cibernética a longo prazo, que começou com a definição de uma metodologia comum de risco, a construção de ferramentas comuns, a implantação da gestão da vulnerabilidade e a monitorização, ensaio e validação do inventário de ativos. Foram realizados progressos neste longo caminho, apesar da complexidade do conjunto de ativos da Comissão, com mais de 1 000 sistemas de informação geridos por mais de 50 direções-gerais e agências de execução.

2. Mecanismos de cooperação das instituições, organismos e agências da UE

A CERT-UE é uma história de sucesso notável na promoção da cooperação não só entre as instituições, organismos e agências da UE, mas também a nível europeu, através da sua participação como membro de pleno direito da rede CSIRT criada ao abrigo da Diretiva SRI. Desta forma, a CERT-UE é um caso exemplar da forma como a cooperação e os serviços de cibersegurança podem ser reforçados. As observações do TCE sobre a CERT-UE ilustram muito claramente o trabalho notável que a CERT-UE está a realizar face a um cenário cada vez mais hostil de ciberameaças e a uma escassez crónica de recursos.

Nos termos do atual Acordo Interinstitucional (AII), as agências descentralizadas e as empresas comuns da UE estão oficialmente representadas no conselho diretivo da CERT-UE pela ENISA. Além disso, os seus pontos de vista são expressos nas reuniões do conselho diretivo por um representante do Comité Consultivo para as TIC (ICTAC), que está autorizado a assistir a ENISA na sua função de representação das agências, mas que não participa formalmente nem tem direito de voto. O nível adequado de representação das agências no comité diretor da CERT-UE será abordado na proposta de regulamento, completando a composição do conselho diretivo com um máximo de três representantes designados pela Rede de Agências da União (EUAN), sob proposta do seu Comité Consultivo para as TIC.

A participação no subgrupo «cibersegurança» do ICDT é feita com base nos melhores esforços, segundo o nível de envolvimento decidido por cada instituição, organismo ou agência da UE. As melhorias em matéria de partilha de informações sobre contratos públicos, enquanto tema importante no âmbito do grupo de trabalho 2 do subgrupo de cibersegurança, estão a ser estudadas na preparação do novo contrato-quadro para a cibersegurança.

No que diz respeito a ferramentas comuns para serviços como o correio eletrónico e a videoconferência, já existe a possibilidade de utilizar o sistema SECEM-2 criado pela Comissão para todas as instituições, organismos e agências da UE para o correio eletrónico cifrado, dependendo da gestão eficaz das chaves e certificados de cifragem. Além disso, está a ser desenvolvida a SECABC, uma ferramenta que permite a cifragem do correio eletrónico entre instituições, com a intenção de oferecer acesso à mesma a todas as instituições, organismos e agências da UE interessados a partir de 2022. A videoconferência segura para os serviços SNC já foi alcançada e pode ser alargada a outras instituições, organismos e agências da UE numa base *ad hoc*, através

da gestão da identidade dos participantes na reunião. A partilha de informações sensíveis será igualmente abordada na proposta de regulamento relativo à segurança da informação (ou seja, através de rótulos e marcações comuns).

3. Partilha de informações sobre incidentes ou vulnerabilidades significativos

O facto de nem todas as instituições, organismos e agências da UE estarem a notificar a CERT-UE de incidentes ou vulnerabilidades significativos é abordado no projeto de regulamento relativo à cibersegurança, em conformidade com a proposta da Comissão de Diretiva SRI-2[1]. O nível de execução dependerá da afetação de recursos adicionais pelas instituições, organismos e agências da UE autónomas. O âmbito de aplicação dessas notificações continua a ser limitado, incluindo no abrigo da atual proposta de regulamento, dada a autonomia institucional das instituições, organismos e agências da UE. A proposta de regulamento relativo à cibersegurança disporá de mecanismos de conformidade adequados e proporcionais ao objetivo e ao âmbito de aplicação das novas regras, sem prejuízo da autonomia das instituições, órgãos e agências.

III. RESPOSTAS DA COMISSÃO ÀS CONCLUSÕES E RECOMENDAÇÕES DO TCE

Recomendação 1 — Melhorar a preparação das instituições, organismos e agências da UE em matéria de cibersegurança através de normas comuns vinculativas e do aumento dos recursos para a CERT-UE

O texto do regulamento proposto incluirá medidas específicas destinadas a aumentar ainda mais o nível comum de cibersegurança. Estas medidas serão traduzidas em planos de cibersegurança, que serão definidos e aplicados ao nível das instituições, organismos e agências da UE no âmbito do seu próprio quadro de governação da cibersegurança.

A Comissão aceita esta recomendação. No que se refere às sub-recomendações específicas, a Comissão observa o seguinte:

a) A Comissão aceita a recomendação 1, alínea a). O projeto de regulamento incluirá disposições sobre os quadros de governação e de controlo, criados ao mais alto nível de gestão executiva de cada instituição, organismo e agência da UE, a fim de assegurar uma gestão eficaz e prudente de todos os riscos de cibersegurança.
b) A Comissão aceita a recomendação 1, alínea b). O projeto de regulamento reforçará a referência à abordagem baseada no risco para a gestão da cibersegurança, tornando claro que as ações, os planos de segurança informática e a execução efetiva dos controlos essenciais devem seguir as avaliações.

[1] Proposta de Diretiva do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e que revoga a Diretiva (UE) 2016/1148, COM(2020) 823 final.

c) A Comissão aceita a recomendação 1, alínea c). Os programas de educação, sensibilização e formação no domínio da cibersegurança serão citados no projeto de regulamento como parte da base de referência em matéria de cibersegurança.
d) A Comissão aceita a recomendação 1, alínea d). De acordo com a nossa experiência, embora as auditorias e os testes regulares sejam essenciais, não são suficientes para garantir a realização de progressos. Por conseguinte, a apresentação regular de relatórios e a transparência são necessárias para o quadro de governação da cibersegurança previsto na alínea a).
e) A Comissão aceita a recomendação 1, alínea e). O projeto de regulamento incluirá disposições relacionadas com a notificação, pelas instituições, organismos e agências da UE, de ciberameaças, vulnerabilidades e incidentes significativos à CERT-UE.
f) A Comissão aceita a recomendação 1, alínea f). A Comissão apoia a necessidade de reforçar os recursos da CERT-UE. As disposições relativas ao pessoal e às contribuições financeiras das instituições, organismos e agências da UE serão incluídas no texto do projeto de regulamento.
g) A Comissão aceita a recomendação 1, alínea g). O regulamento proposto disporá de mecanismos de conformidade proporcionais ao objetivo e ao âmbito das disposições, no respeito da autonomia institucional das instituições, organismos e agências da UE. O conteúdo do futuro regulamento depende do resultado do processo legislativo e da decisão dos legisladores da UE relativamente à proposta apresentada pela Comissão.

Recomendação 2 — Promover mais sinergias entre as instituições, organismos e agências da UE em áreas selecionadas

A Comissão, que preside atualmente ao subgrupo «cibersegurança» do Comité Interinstitucional para a Transformação Digital (ICDT), concorda com as recomendações no sentido de promover soluções para a partilha coerente e segura de informações sensíveis, a partilha sistemática de informações sobre projetos de cibersegurança e quadros comuns de contratação pública de serviços de cibersegurança.

A Comissão aceita esta recomendação. No que se refere às sub-recomendações específicas, a Comissão observa o seguinte:

a) A Comissão aceita a recomendação 2, alínea a). A Comissão está a propor iniciativas e serviços técnicos ao subgrupo «cibersegurança» do ICDT, a fim de promover e apoiar ferramentas comuns para a partilha de informações sensíveis, permitindo serviços como o correio eletrónico e a videoconferência. O Tribunal observa igualmente que as marcações comuns e as regras comuns de tratamento das informações sensíveis não classificadas serão abordadas na proposta de regulamento relativo à segurança das informações.
b) A Comissão aceita a recomendação 2, alínea b). Os grupos de trabalho existentes no âmbito do subgrupo «cibersegurança» do ICDT estão a abordar este ponto, que será desenvolvido mais aprofundadamente. As melhorias em matéria de partilha de informações em matéria de contratos públicos estão a ser abordadas na preparação do novo contrato-quadro para a cibersegurança.
c) A Comissão aceita a recomendação 2, alínea c). As instituições, organismos e agências da UE já têm acesso a contratos-quadro interinstitucionais no domínio das TIC geridos pela Comissão. A preparação do novo contrato-quadro para a cibersegurança será coordenada com o subgrupo «cibersegurança» do ICDT.

Recomendação 3 — Aumentar o foco da CERT-UE e da ENISA nas instituições, organismos e agências da UE com menos maturidade

Os destinatários desta recomendação são a CERT-UE e a ENISA.