PT 2022

05

Relatório especial

Cibersegurança das instituições, organismos e agências da UE

Em geral, o nível de preparação não é proporcional às ameaças

TRIBUNAL
DE CONTAS
EUROPEU

Índice

Síntese

I O Regulamento Cibersegurança da UE define a cibersegurança como "as atividades necessárias para proteger a rede e os sistemas de informação, os utilizadores desses sistemas e outras pessoas afetadas pelas ciberameaças". Devido às informações sensíveis que processam, as instituições, organismos e agências da UE (EUIBA) são alvos atrativos para potenciais atacantes, especialmente para os grupos com capacidade de realizar ataques furtivos altamente sofisticados para fins de ciberespionagem e outros. Apesar da sua independência institucional e autonomia administrativa, as EUIBA estão fortemente interligadas, pelo que as fragilidades de uma podem expor outras a ameaças à segurança.

II Uma vez que o número de ciberataques contra as EUIBA está a aumentar acentuadamente, o objetivo da presente auditoria foi determinar se as EUIBA, em geral, estabeleceram mecanismos adequados para se protegerem contra as ciberameaças. O Tribunal conclui que o conjunto das EUIBA não alcançou um nível de preparação cibernética compatível com as ameaças.

III O Tribunal constatou que as boas práticas fundamentais em matéria de cibersegurança, incluindo alguns controlos essenciais, nem sempre foram seguidas, e que várias EUIBA apresentam despesas claramente insuficientes no domínio da cibersegurança. De igual modo, a boa governação em matéria de cibersegurança não foi ainda posta em prática em algumas EUIBA: as estratégias de segurança informática são, em muitos casos, inexistentes ou não são aprovadas pelos quadros superiores; as políticas de segurança nem sempre são formalizadas; e as avaliações de riscos não abrangem todo o ambiente informático. Nem todas as EUIBA submetem regularmente a sua cibersegurança à prestação de uma garantia independente.

IV A formação em cibersegurança nem sempre é sistemática. Pouco mais de metade das EUIBA oferece formação contínua sobre cibersegurança ao pessoal da informática e aos especialistas em segurança informática, e poucas EUIBA fornecem formação obrigatória em matéria de cibersegurança aos dirigentes responsáveis por sistemas informáticos que contêm informações sensíveis. Os exercícios de *phishing* são uma ferramenta importante para formar e sensibilizar o pessoal, mas nem todas as EUIBA os utilizam de forma sistemática.

V Embora as EUIBA tenham estabelecido estruturas para a cooperação e o intercâmbio de informações em matéria de cibersegurança, o Tribunal observou que as potenciais sinergias não são totalmente exploradas. As EUIBA não partilham sistematicamente entre si informações sobre projetos relacionados com a cibersegurança, avaliações de segurança e contratos de prestação de serviços. Além disso, ferramentas de comunicação básicas, como o correio eletrónico encriptado ou as soluções utilizadas para a realização de videoconferências, não são totalmente interoperáveis, o que pode resultar na menor segurança das trocas de informações, numa duplicação de esforços e num aumento dos custos.

VI A Equipa de Resposta a Emergências Informáticas para as instituições e agências da UE (CERT-UE) e a Agência da União Europeia para a Cibersegurança (ENISA) são as duas principais entidades responsáveis pelo apoio às EUIBA no domínio da cibersegurança. No entanto, devido a limitações de recursos ou à atribuição de prioridade a outras áreas, não conseguiram prestar às EUIBA todo o apoio de que estas necessitam, especialmente no tocante ao desenvolvimento de capacidades nas EUIBA com menos maturidade. Embora a CERT-UE seja altamente valorizada pelas EUIBA, a sua eficácia é prejudicada pelo aumento da carga de trabalho, a instabilidade em termos de financiamento e de pessoal e por uma cooperação insuficiente por parte de algumas EUIBA, que nem sempre partilham atempadamente informações sobre vulnerabilidades e ciberincidentes significativos que as tenham afetado ou possam afetar outras EUIBA.

VII Com base nestas conclusões, o Tribunal recomenda que:

- a Comissão deve promover a melhoria do nível de preparação de todas as EUIBA em matéria de cibersegurança através de uma proposta legislativa que introduza regras vinculativas comuns neste domínio para todas e do aumento de recursos da CERT-UE;

- a Comissão, no contexto do Comité Interinstitucional para a Transformação Digital, deve promover novas sinergias entre as EUIBA em áreas selecionadas;

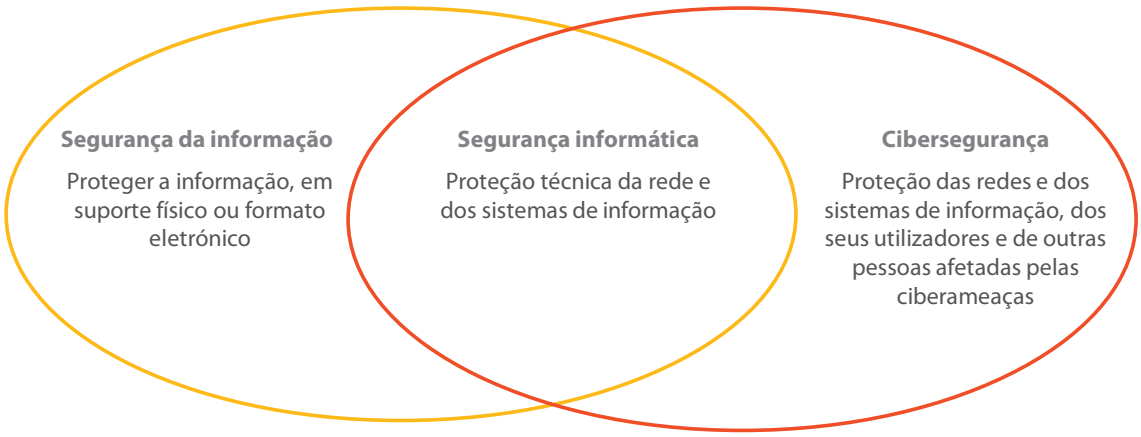
- a CERT-UE e a ENISA devem centrar-se mais nas EUIBA que apresentam menos maturidade no domínio da cibersegurança;

Introdução

O que é a cibersegurança?

01 O Regulamento Cibersegurança da UE[1] define a cibersegurança como "as atividades necessárias para proteger a rede e os sistemas de informação, os utilizadores desses sistemas e outras pessoas afetadas pelas ciberameaças". A cibersegurança assenta na segurança da informação, que consiste em preservar a confidencialidade, a integridade e a disponibilidade das informações[2], quer em suporte físico quer em formato eletrónico. Além disso, a proteção da rede e dos sistemas de informação onde essas informações se encontram armazenadas é conhecida como segurança das tecnologias da informação (TI) (ver ***figura 1***).

Figura 1 – A cibersegurança está associada à segurança da informação e à segurança informática



Fonte: TCE.

02 Como disciplina, a cibersegurança envolve a identificação, prevenção, deteção e resposta a ciberincidentes, bem como a recuperação dos mesmos. Os incidentes podem ir, por exemplo, da divulgação acidental de informações a ataques destinados a comprometer infraestruturas críticas e ao roubo de identidades e de dados pessoais[3].

---

[1] Regulamento (UE) 2019/881.

[2] ISO/IEC 27000:2018.

[3] TCE, Documento de análise 02/2019: *Desafios à eficácia da política de cibersegurança da UE* (Documento informativo).

03 Um quadro de cibersegurança é composto por muitos elementos, incluindo requisitos e controlos técnicos para a segurança da rede e dos sistemas de informação, bem como disposições de governação adequadas e programas de sensibilização para a cibersegurança destinados ao pessoal.

Cibersegurança das instituições, organismos e agências da UE

04 Devido à informação sensível que processam, as instituições, organismos e agências da UE (EUIBA) são alvos atrativos para os potenciais atacantes, especialmente os grupos capazes de realizar ataques furtivos altamente sofisticados ("ameaças persistentes avançadas") para fins de ciberespionagem e outros[4]. Os ciberataques bem-sucedidos contra as EUIBA podem ter implicações políticas significativas, prejudicar a reputação geral da UE e minar a confiança nas suas instituições.

05 A pandemia de COVID-19 obrigou as EUIBA, à semelhança de muitas outras organizações em todo o mundo, a acelerarem abruptamente a transformação digital e a aderirem ao trabalho à distância. Esta situação aumentou consideravelmente o número de pontos de acesso potenciais para os atacantes (a "superfície de ataque"), alargando o perímetro de cada organização a casas e dispositivos móveis ligados à Internet, onde podem ser exploradas novas vulnerabilidades. Os serviços de acesso remoto são uma das vias mais comuns através das quais os grupos que visam as EUIBA com ameaças persistentes avançadas obtêm acesso inicial às suas redes.[5]

06 O número de ciberincidentes está a crescer e o aumento drástico de incidentes significativos que afetam as EUIBA[6], e que fez de 2021 um ano recorde, é uma tendência particularmente preocupante. Classificam-se como incidentes significativos aqueles cuja natureza não é nem repetitiva nem básica. Normalmente, implicam a utilização de novos métodos e tecnologias, e a investigação e recuperação dos mesmos pode levar semanas ou, até, meses. Os incidentes significativos aumentaram mais de dez vezes entre 2018 e 2021[7]. Só nos últimos dois anos, pelo menos 22 EUIBA individuais foram afetadas por incidentes significativos. Um exemplo recente foi o

---

[4] CERT-UE, *Threat Landscape Report*, junho de 2021.

[5] *Ibid*.

[6] *Ibid*.

[7] *Ibid*.

ciberataque à Agência Europeia de Medicamentos, em que dados sensíveis foram divulgados e manipulados com vista a comprometer a confiança nas vacinas[8].

07 As EUIBA são um grupo muito heterogéneo, composto por instituições, agências e vários organismos diferentes. As sete instituições da UE foram criadas pelos Tratados. As agências descentralizadas da UE, bem como outros organismos, foram criadas por atos de direito derivado e são entidades jurídicas distintas. Existem diferentes tipos jurídicos de agências: seis agências de execução da Comissão e 37 agências descentralizadas da UE[9]. As EUIBA incluem também gabinetes da UE, um corpo diplomático (o Serviço Europeu para a Ação Externa), empresas comuns e outros organismos. Cada uma das EUIBA é responsável pela definição dos seus próprios requisitos de cibersegurança e pela execução das suas próprias medidas de segurança.

08 Para reforçar a cibersegurança das EUIBA, em 2012 a Comissão criou a Equipa de Resposta a Emergências Informáticas para as instituições e agências da UE (CERT-UE) na qualidade de grupo de trabalho permanente. A CERT-UE funciona para as EUIBA como uma plataforma de intercâmbio de informações sobre cibersegurança e de coordenação da resposta a incidentes e coopera com outras equipas de resposta a incidentes de segurança informática (CSIRT) nos Estados-Membros e com empresas especializadas em segurança informática. Atualmente, o funcionamento e a organização da CERT-UE são regidos por um acordo interinstitucional[10] (AII) celebrado em 2018 entre as EUIBA que a CERT-UE serve, também designadas como "as partes", que presentemente são 87.

09 Outro interveniente fundamental que apoia as EUIBA é a Agência da União Europeia para a Cibersegurança (ENISA), cujo propósito é alcançar um elevado nível comum de cibersegurança em toda a UE. Criada em 2004, a ENISA tem por missão reforçar a fiabilidade dos produtos, processos e serviços das tecnologias da informação e comunicação (TIC) com esquemas de certificação de cibersegurança, bem como cooperar com as EUIBA e os Estados-Membros e ajudá-los a prepararem-se para as ciberameaças. A ENISA apoia as EUIBA no desenvolvimento de capacidades e na cooperação operacional.

---

[8] *Cyberattack on EMA – update 6*, 25.1.2021.

[9] Relatório especial 22/2020 do TCE, *Futuro das agências da UE – potencial para maior flexibilidade e cooperação*, ponto 1.

[10] JO C 12, de 13.1.2018, p. 1.

10 Pese embora a sua independência institucional, as EUIBA estão fortemente interligadas. Trocam informações diariamente e partilham diversos sistemas e redes comuns. As fragilidades de uma EUIBA podem expor outras a ameaças à segurança, uma vez que muitos ciberataques incluem mais do que uma etapa para atingir o seu objetivo ou alvo final[11]. Um ataque bem-sucedido contra uma EUIBA mais vulnerável pode ser utilizado como ponto de partida para atingir outras. Há também uma interligação entre as EUIBA e organizações públicas e privadas dos Estados-Membros. Se as EUIBA não estiverem suficientemente bem preparadas para lidar com ciberameaças, podem, por conseguinte, expor estas organizações.

11 Atualmente, não há um quadro jurídico para a segurança da informação e a cibersegurança nas EUIBA. Estes domínios não estão sujeitos à legislação mais ampla da UE em matéria de cibersegurança, a Diretiva SRI de 2016[12], nem à sua proposta de revisão, a Diretiva SRI revista[13]. Tampouco existem informações exaustivas sobre o montante gasto pelas EUIBA em cibersegurança.

12 Em julho de 2020, a Comissão publicou uma comunicação sobre a Estratégia da EU para a União da Segurança[14] para o período de 2020-2025. As suas ações-chave incluem "regras comuns em matéria de segurança da informação e de cibersegurança para todas as EUIBA". Este novo quadro destina-se a sustentar uma cooperação operacional sólida e eficiente centrada na função da CERT-UE. Na Estratégia de Cibersegurança da UE para a Década Digital[15], publicada em dezembro de 2020, a Comissão comprometeu-se a propor um regulamento sobre regras comuns de cibersegurança para todas as EUIBA. Propôs, igualmente, o estabelecimento de uma nova base jurídica para a CERT-UE a fim de reforçar o seu mandato e financiamento.

---

[11] ENISA, *Threat Landscape 2020, Sectoral/thematic threat analysis*.

[12] 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.

[13] Proposta de diretiva relativa a medidas destinadas a assegurar um elevado nível comum de cibersegurança na União.

[14] COM(2020) 605 final.

[15] JOIN(2020) 18 final.

Âmbito e método da auditoria

13 Uma vez que o número de ciberataques está a aumentar acentuadamente e que as fragilidades de uma EUIBA podem expor outras a ameaças à segurança, o objetivo da presente auditoria foi determinar se as EUIBA, no seu conjunto, estabeleceram mecanismos adequados para se protegerem contra as ciberameaças. Para responder a esta questão principal de auditoria, o Tribunal colocou três subquestões:

1) as principais práticas de cibersegurança são adotadas em todas as EUIBA?

2) existe uma cooperação eficiente entre as EUIBA em matéria de cibersegurança?

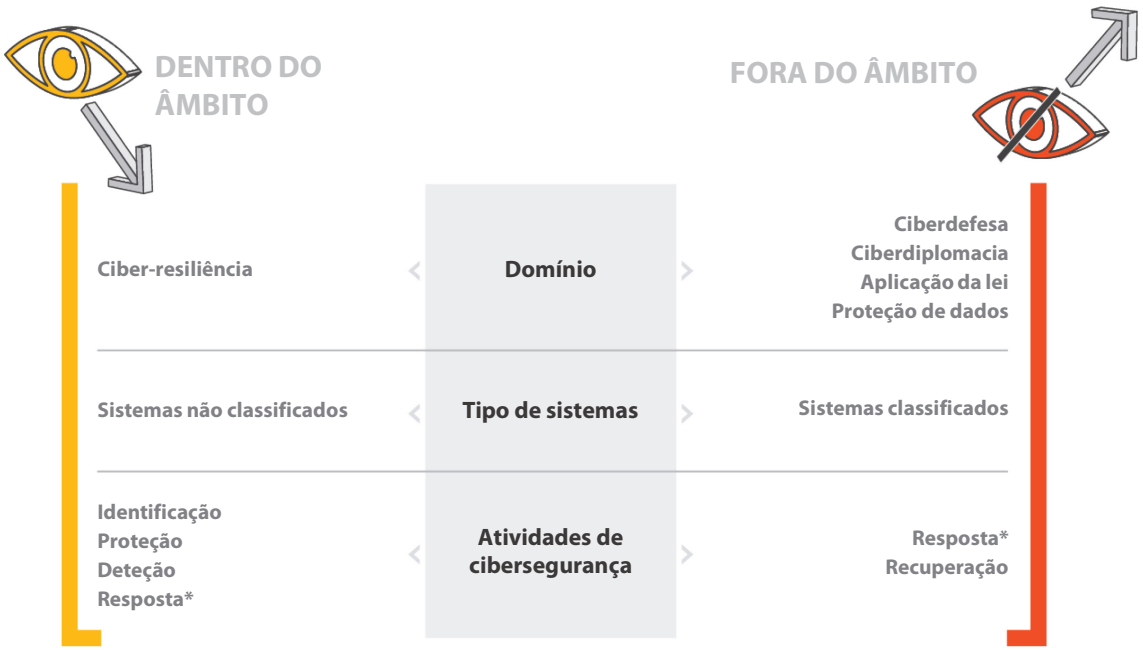
3) a ENISA e a CERT-UE prestam um apoio adequado às EUIBA no domínio da cibersegurança?

14 O calendário da auditoria está alinhado com a Estratégia para a União da Segurança. Ao avaliar as atuais disposições das EUIBA em matéria de cibersegurança, o Tribunal pretende assinalar as áreas a melhorar, que a Comissão pode considerar aquando da elaboração da sua proposta legislativa relativa a regras de cibersegurança comuns vinculativas para todas as EUIBA.

15 A auditoria abrangeu evoluções e iniciativas na área da cibersegurança entre janeiro de 2018 (altura em que foi estabelecido o acordo interinstitucional CERT-UE) e outubro de 2021.

16 O Tribunal limitou o seu âmbito de auditoria à ciber-resiliência e aos sistemas não classificados e centrou-se nos aspetos relacionados com a preparação (atividades correspondentes à "identificação, proteção, deteção"). A "resposta" e a "recuperação" estavam fora do âmbito do Tribunal. No entanto, foram examinados alguns elementos organizacionais de resposta a incidentes. Os aspetos relacionados com a proteção de dados, aplicação da lei, ciberdefesa e ciberdiplomacia estão também fora do âmbito do Tribunal (ver ***figura 2***).

Figura 2 – Âmbito da auditoria



** Foram examinados apenas alguns aspetos organizacionais da resposta a incidentes. Outros aspetos estavam fora do âmbito da auditoria.*

Fonte: TCE.

17 As constatações de auditoria do Tribunal baseiam-se numa análise exaustiva da documentação disponível, complementada por entrevistas. O Tribunal realizou um inquérito de autoavaliação que envolveu 65 EUIBA, com vista a recolher informações sobre as suas disposições em matéria de cibersegurança e os seus pontos de vista sobre a cooperação interinstitucional. O Tribunal inquiriu todas as EUIBA abrangidas pelos direitos de auditoria do TCE e que gerem a sua própria infraestrutura informática, bem como o próprio TCE. As EUIBA abrangidas incluíram instituições, agências descentralizadas, empresas comuns e organismos. O Tribunal inquiriu igualmente as missões civis, que são entidades autónomas temporárias financiadas pelo orçamento da UE e independentes em termos de TI. O ***anexo 1*** apresenta uma lista completa das EUIBA inquiridas. O Provedor de Justiça Europeu e a Autoridade Europeia para a Proteção de Dados não foram abrangidos no âmbito da presente auditoria.

18 O inquérito teve uma taxa de resposta de 100% e serviu de ponto de partida para uma análise mais aprofundada. Além disso, o Tribunal selecionou uma amostra de sete EUIBA que é representativa da heterogeneidade das mesmas e deu seguimento às suas respostas através de entrevistas e pedidos de documentação. Os critérios de seleção considerados compreendiam a base jurídica, a dimensão (em termos de pessoal e de orçamento) e o setor. A amostra de EUIBA era constituída pela Comissão Europeia, o Parlamento Europeu, a Agência da UE para a Cibersegurança (ENISA), a

Autoridade Bancária Europeia (EBA), a Agência Europeia da Segurança Marítima (EMSA), a Missão de Aconselhamento da União Europeia sobre a Reforma do Setor da Segurança Civil na Ucrânia (EUAM Ucrânia) e a Empresa comum para a execução da iniciativa tecnológica conjunta sobre medicamentos inovadores (Empresa Comum IMI).

19 O Tribunal realizou igualmente videoconferências com a CERT-UE, o Comité Consultivo de TIC da rede de Agências (ICTAC), o Comité Interinstitucional para a Transformação Digital (ICDT) e outras partes interessadas pertinentes.

Observações

As EUIBA têm níveis muito diferentes de maturidade em matéria de cibersegurança e não cumprem sempre as boas práticas

20 A presente secção analisa as disposições individuais e os quadros de cibersegurança das EUIBA. O Tribunal avaliou se as EUIBA lidam com a cibersegurança de forma coerente e adequada em termos de governação da segurança informática, gestão de riscos, atribuição de recursos, formação para a sensibilização, controlos e garantia independente.

A governação da segurança informática nas EUIBA não está, muitas vezes, bem desenvolvida, e as avaliações de riscos não são exaustivas

Existem lacunas na governação da segurança informática em muitas EUIBA

21 A boa governação desempenha um papel essencial num quadro eficaz para a segurança da informação e dos sistemas informáticos, uma vez que define os objetivos da organização e fornece orientações através da definição de prioridades e da tomada de decisões. De acordo com a Information Systems Audit and Control Association (ISACA)[16], um quadro de governação da segurança informática deve, em geral, incluir vários elementos:

- uma estratégia de segurança abrangente intrinsecamente ligada aos objetivos empresariais;
- políticas de segurança de governação que abordem cada aspeto da estratégia, dos controlos e do regulamento;
- um conjunto completo de normas para cada política que descreva as medidas operacionais necessárias para o cumprimento da política;
- processos de acompanhamento institucionalizados com vista a garantir a conformidade e a proporcionar retorno sobre a eficácia;
- uma estrutura organizacional eficaz sem conflitos de interesses.

[16] ISACA, *Certified Information System Auditor review manual*, 2019.

22 O Tribunal detetou insuficiências na governação da segurança informática em muitas EUIBA. Apenas 58% das EUIBA (38 em 65) têm uma estratégia de segurança informática ou, pelo menos, um plano de segurança informática aprovado a nível do conselho de administração/quadros superiores. Uma desagregação por tipo de EUIBA revela que as missões civis e as agências descentralizadas (que, no seu conjunto, representam 71% das EUIBA inquiridas) apresentam as percentagens mais baixas (ver ***quadro 1***). A ausência de uma estratégia de segurança informática ou de um plano de segurança informática aprovado a nível dos quadros superiores implica o risco de estes não terem conhecimento das questões de segurança informática ou de não lhes darem prioridade suficiente.

Quadro 1 – Percentagem de EUIBA com uma estratégia ou plano de segurança informática aprovados pelos quadros superiores

Desagregação por número de efetivos

< 100 efetivos (22 EUIBA)	100 a 249 efetivos (17 EUIBA)	250 a 1 000 efetivos (16 EUIBA)	>1 000 efetivos (10 EUIBA)
45%	53%	69%	80%

Desagregação por tipo de EUIBA

Agências descentralizadas (35 EUIBA)	Missões civis (11 EUIBA)	Organismos (4 EUIBA)	Instituições (6 EUIBA)	Empresas Comuns (9 EUIBA)
45%	56%	75%	83%	89%

Fonte: inquérito do TCE.

23 O Tribunal examinou as estratégias/os planos de segurança informática fornecidos pelas sete EUIBA incluídas na amostra (ver ponto ***18***). Constatou que as estratégias das EUIBA estão razoavelmente bem associadas aos objetivos das organizações. Por exemplo, a estratégia de segurança informática da Comissão abrange a dimensão de segurança informática da Estratégia Digital da Comissão Europeia[17] e destina-se a apoiar o seu roteiro e os seus objetivos. No entanto, apenas três EUIBA incluídas na amostra do Tribunal tinham incluído nas suas estratégias/planos de segurança informática objetivos concretos e um calendário para a sua realização.

[17] Comunicação à Comissão, Estratégia digital da Comissão Europeia: *A digitally transformed, user-focused and data-driven Commission*, C(2018) 7118 final, de 21.11.2018.

24 As políticas de segurança estabelecem as regras e os procedimentos que os indivíduos que utilizam ou gerem as informações e os recursos informáticos devem seguir. Ajudam a atenuar os riscos em matéria de cibersegurança e informam sobre as medidas a tomar em caso de incidentes. O Tribunal constatou que 78% das EUIBA têm uma política formal de segurança da informação, enquanto apenas 60% dispõem de políticas formais de segurança informática (ver ***figura 1*** para conhecer as definições de segurança da informação e segurança informática). O Tribunal constatou também que quatro das sete EUIBA incluídas na amostra têm políticas de segurança consentâneas com as suas estratégias de segurança informática. No entanto, em três destas quatro EUIBA, as políticas de segurança informática são apenas parcialmente complementadas por normas de segurança pormenorizadas e atualizadas que descrevem as medidas operacionais necessárias para executar as políticas. A falta de normas de segurança formais aumenta o risco de as questões de segurança informática não serem tratadas de forma adequada e coerente dentro da mesma EUIBA. Além disso, dificulta a avaliação da conformidade da organização com a sua política de segurança informática. Das sete EUIBA incluídas na amostra, apenas a Comissão dispõe de procedimentos estruturados para acompanhar a conformidade com as suas políticas e normas de segurança informática, embora estes apenas sejam utilizados por um número limitado de Direções-Gerais (DG) (ver ***caixa 1***).

Caixa 1

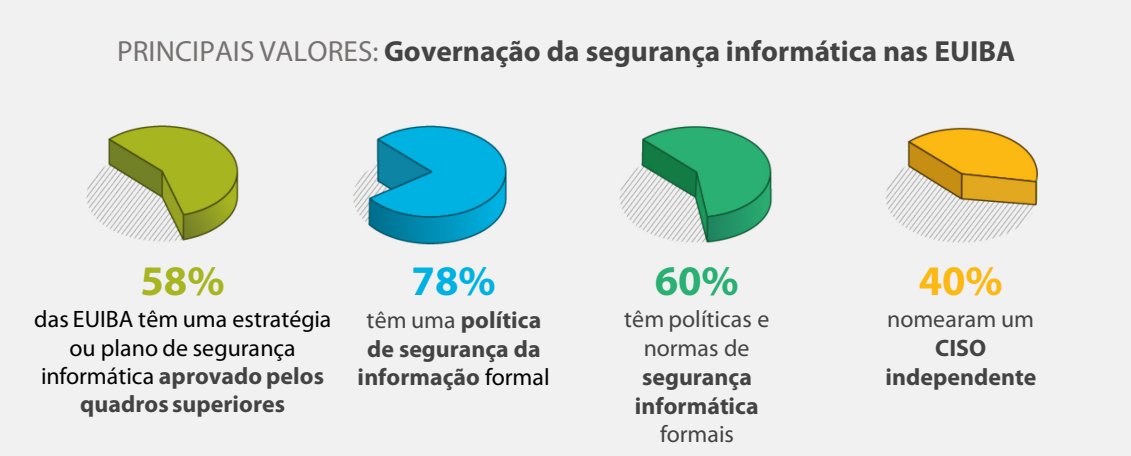
Conformidade com a segurança informática na Comissão

Em conformidade com a governação descentralizada das TI na Comissão, o chefe de cada DG é o proprietário do serviço responsável pelo cumprimento das normas de segurança informática por parte dos seus sistemas. A Direção-Geral da Informática (DG DIGIT) e a Direção-Geral dos Recursos Humanos e da Segurança (DG Recursos Humanos e Segurança) acompanham e facilitam a execução das práticas de gestão da conformidade. A DG DIGIT criou uma ferramenta (conhecida como "GRC") que permite às DG avaliar e comunicar informações sobre a sua conformidade com os controlos da política de segurança informática.

Os 580 controlos estão divididos em três grupos: controlos gerais (a maioria em matéria de governação), controlos específicos das DG e controlos específicos do sistema. A ferramenta está operacional, mas, até à data, apenas cinco DG a utilizam. Por conseguinte, a DG DIGIT não tem uma visão global da conformidade em toda a Comissão. No entanto, o Conselho das Tecnologias da Informação e da Cibersegurança (ITCB) da Comissão pode solicitar à DG DIGIT que investigue a conformidade com uma norma específica (por exemplo, autenticação de dois fatores em 2021) e pode emitir pareceres e recomendações não vinculativos, bem como requisitos formais, no caso de riscos críticos.

25 Outro elemento importante na boa governação da cibersegurança é a nomeação de um Diretor da Segurança da Informação (CISO). Embora não seja explicitamente exigida pelo conjunto de normas ISO 27000[18], a existência de um CISO ou de um cargo equivalente tornou-se uma prática generalizada entre organizações e faz parte das orientações da ISACA. Em regra, o CISO é globalmente responsável pelos programas de segurança informática e de segurança da informação da organização. Para evitar qualquer conflito de interesses, o CISO deve ter um determinado grau de independência em relação à função/ao serviço de TI[19].

26 De acordo com o inquérito do Tribunal, 60% das EUIBA não nomearam um CISO independente nem uma função equivalente. Mesmo quando são nomeados CISO (ou cargos equivalentes), as suas responsabilidades diferem consideravelmente em termos de natureza – e as suas funções são entendidas de forma diferente – entre as EUIBA. Especialmente nas EUIBA de pequena e média dimensão, os CISO tendem a estar associados a funções mais operacionais, não funcionalmente independentes do serviço de TI. Esta situação pode limitar a autonomia dos CISO na execução das suas prioridades em matéria de segurança. A ENISA está atualmente a trabalhar num quadro da UE de aptidões em matéria de cibersegurança, que visa, nomeadamente, criar um entendimento comum de funções, competências e aptidões.



As avaliações dos riscos de segurança informática das EUIBA, na maioria, não abrangem a globalidade do seu ambiente informático

27 Todas as normas internacionais relativas à segurança informática sublinham a importância de se estabelecer um método adequado para avaliar e gerir os riscos de

[18] Norma ISO/IEC 27000:2018, capítulo 5.

[19] COBIT 5 para a Segurança da informação, secção 4.2.

segurança que afetam os sistemas informáticos e os dados que estes contêm. As avaliações de riscos devem ser realizadas periodicamente, para analisar as alterações dos requisitos de segurança da informação de uma organização e os riscos que esta enfrenta[20]. As avaliações devem ser seguidas de um plano de atenuação dos riscos (ou de um plano de segurança informática).

28 A maioria das EUIBA inquiridas (58 em 65) indicou que segue um quadro ou uma metodologia para a realização de avaliações de riscos nos seus sistemas informáticos. No entanto, não existe uma metodologia comum transversal a todas as EUIBA. Pelo menos 26 EUIBA utilizam parcial ou totalmente as metodologias desenvolvidas pela Comissão. Em concreto, 31% das EUIBA utilizaram a metodologia de gestão dos riscos de segurança informática de 2018 (ITSRM2). As outras seguem metodologias baseadas em normas bem conhecidas da indústria (como a ISO 27001, ISO 27005, o quadro de cibersegurança do Instituto Nacional de Normas e Tecnologias (NIST-CSF) ou os controlos do Center for Internet Security (CIS)) ou utilizam outras metodologias internas.

29 Das sete EUIBA incluídas na amostra, apenas duas realizam avaliações de riscos exaustivas que abrangem todo o seu ambiente informático (ou seja, todos os seus sistemas informáticos). A maioria efetua apenas avaliações de riscos individuais relativamente aos seus sistemas informáticos mais importantes. O Tribunal constatou vários exemplos de avaliações de riscos realizadas antes da instalação de novos sistemas. No entanto, não foram encontradas provas de avaliações de riscos de seguimento relacionadas, por exemplo, com alterações subsequentes dos sistemas/infraestruturas.

O tratamento da cibersegurança pelas EUIBA nem sempre é consistente, e os controlos essenciais nem sempre estão em vigor

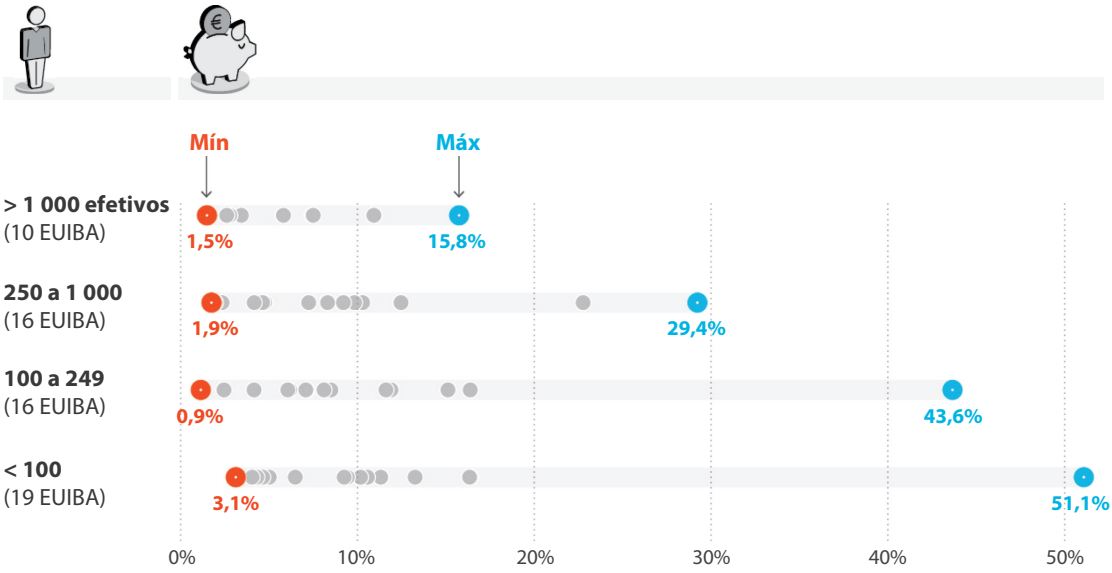
A atribuição de recursos à cibersegurança varia amplamente entre as EUIBA

30 No inquérito do Tribunal, foi solicitado às EUIBA que apresentassem o total das suas despesas em TI em 2020 e uma estimativa do montante gasto em cibersegurança. Os dados do Tribunal revelam variações significativas na percentagem de despesas em TI que as EUIBA individuais atribuem à cibersegurança. Esta situação verifica-se inclusivamente entre EUIBA de dimensão semelhante em termos do número de

[20] Ver, por exemplo, a Norma ISO/IEC 27000:2018, secção 4.5.

efetivos. Conforme ilustrado na ***figura 3***, as diferenças tendem a ser particularmente elevadas entre as EUIBA com menos pessoal.

Figura 3 – Despesas de cibersegurança como percentagem do total de despesas em TI (EUIBA agrupadas pelo número de efetivos)



Nota: quatro EUIBA não facultaram dados sobre as despesas em cibersegurança.

Fonte: inquérito do TCE.

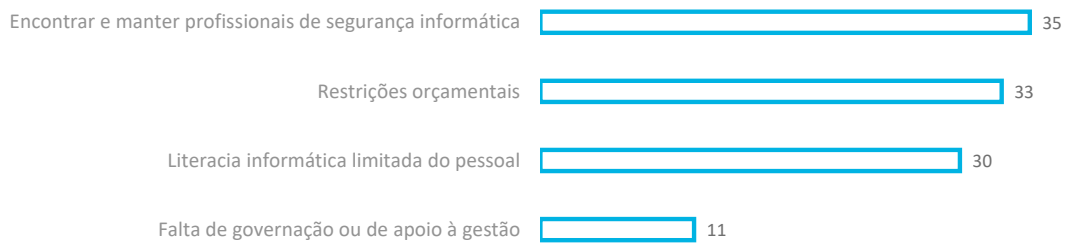
31 É difícil avaliar um nível ideal de despesa em cibersegurança em termos absolutos, pois este depende de muitos fatores, como a superfície de ataque da organização, a sensibilidade dos dados que esta trata, o seu perfil e apetência pelo risco e os requisitos jurídicos/regulamentares setoriais. No entanto, os dados do Tribunal destacam que as diferenças são substanciais e que as razões desta discrepância nem sempre são óbvias. Algumas EUIBA têm despesas em cibersegurança consideravelmente inferiores aos seus pares de dimensão comparável, as quais poderão revelar-se insuficientes no caso de essas entidades serem expostas a ameaças e riscos semelhantes.

32 A maioria das EUIBA são de pequena a média dimensão tanto em termos de pessoal como de despesas em TI, tendo dois terços delas menos de 350 efetivos. A EUIBA de menor dimensão tem apenas 15 efetivos. A gestão da cibersegurança é mais desafiante e exige mais recursos para as EUIBA de menor dimensão. Na maioria dos casos, não podem beneficiar de economias de escala e não dispõem de saber-fazer interno suficiente. Com base no inquérito e nas entrevistas do Tribunal, as maiores instituições, como a Comissão e o Parlamento Europeu, dispõem de equipas de especialistas que gerem a cibersegurança a tempo inteiro. No entanto, nas EUIBA de menor dimensão, onde o pessoal e os recursos são particularmente limitados, não

existem especialistas e a cibersegurança é gerida a tempo parcial por pessoal com conhecimentos de TI. Uma vez que as EUIBA estão fortemente interligadas, esta situação representa um risco acrescido (ver também o ponto ***10***).

33 No inquérito do Tribunal, as EUIBA foram questionadas relativamente aos principais desafios na execução de políticas de cibersegurança eficazes nas respetivas organizações (ver ***figura 4***). O maior deles reside no facto de os especialistas em cibersegurança serem um recurso escasso e de muitas EUIBA terem dificuldade em atraí-los, devido à concorrência tanto do setor privado, como de outras EUIBA. Os problemas recorrentes incluem procedimentos de recrutamento morosos, condições contratuais não competitivas e a falta de perspetivas de carreira atrativas. A escassez de pessoal especializado representa um risco significativo para o tratamento eficaz da cibersegurança.

Figura 4 – Desafios na aplicação de políticas de cibersegurança eficazes nas EUIBA (podia ser selecionado mais do que um fator)



Fonte: inquérito do TCE.

A maioria das EUIBA oferece algum tipo de formação para a sensibilização em matéria de cibersegurança, mas não de modo sistemático nem bem direcionado

34 Tirar partido das vulnerabilidades dos sistemas e dispositivos não é a única forma de os potenciais atacantes causarem danos. Estes podem também induzir os utilizadores a revelar informações sensíveis ou a descarregar *software* malicioso, por exemplo, através de *phishing* ou de engenharia social. O pessoal faz parte da primeira linha de defesa de todas as organizações. Por conseguinte, os programas de formação e de sensibilização para a cibersegurança são um elemento fundamental num quadro eficaz em matéria de cibersegurança.

35 A grande maioria das EUIBA inquiridas (9%) oferece algum tipo de formação geral de sensibilização para a cibersegurança a todo o pessoal, mas três não o fazem. No entanto, apenas 41% das EUIBA organizam sessões de formação ou de sensibilização específicas para os dirigentes e apenas 29% oferecem formação obrigatória em

matéria de cibersegurança aos dirigentes responsáveis por sistemas informáticos que contêm informações sensíveis. A sensibilização e o empenho da administração são cruciais para uma governação eficaz em matéria de cibersegurança. Das onze EUIBA que mencionaram a falta de apoio à administração como um desafio para uma cibersegurança eficaz, apenas três ofereceram alguma formação para a sensibilização aos seus dirigentes. A formação contínua sobre cibersegurança para o pessoal da informática e os especialistas em segurança informática é oferecida por, respetivamente, 58% e 51% das EUIBA.

36 Nem todas as EUIBA dispõem de mecanismos para acompanhar a participação do pessoal na formação em cibersegurança e a subsequente mudança no seu nível de sensibilização e comportamento. Especialmente nas organizações de menor dimensão, as sessões de sensibilização para a cibersegurança podem ser oferecidas no contexto de reuniões informais do pessoal. A principal forma de as organizações avaliarem a sensibilização do pessoal é através de testes periódicos ao seu comportamento, incluindo mediante inquéritos sobre a maturidade ou exercícios de *phishing.* Nos últimos cinco anos, 55% das EUIBA organizaram uma ou mais campanhas de simulação de *phishing* (ou exercícios semelhantes). Uma vez que o *phishing* é uma das principais ameaças que o pessoal das administrações públicas enfrenta[21], estes exercícios são uma ferramenta importante para formar e sensibilizar o pessoal. O Tribunal considerou que as ações de sensibilização para a cibersegurança da Comissão constituem uma boa prática e estão à disposição de outras EUIBA interessadas (ver ***caixa 2***).

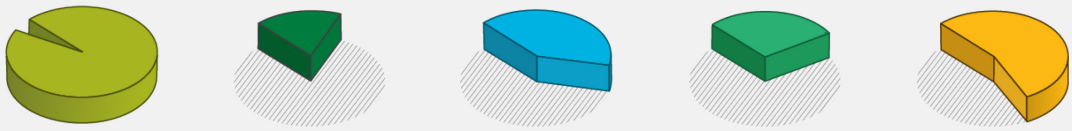
[21] ENISA, *Thread Landscape 2020*, *Sectoral/Thematic threat analysis*.

Caixa 2

Formação para a sensibilização em matéria de cibersegurança na Comissão

A Comissão tem uma equipa específica designada "*Cyber Aware*" na DG DIGIT que lidera o programa institucional de sensibilização para a cibersegurança. O programa é gerido e executado em conjunto com a DG Recursos Humanos e Segurança, o Secretariado-Geral, a Direção-Geral das Redes de Comunicação, Conteúdos e Tecnologias (DG CNECT) e a CERT-UE. A formação é de elevada qualidade e, em muitos casos, tem um alcance interinstitucional. As sessões de formação são anunciadas através de um boletim dedicado à aprendizagem (*Learning Bulletin*), que chega a cerca de 65 000 efetivos da UE. Através da plataforma "Cyber Aware", a Comissão organizou 15 exercícios de *phishing* nos últimos cinco anos e, recentemente, realizou o primeiro exercício à escala da Comissão.

PRINCIPAIS VALORES: **Formação para a sensibilização em matéria de cibersegurança nas EUIBA**



95% disponibilizam ao pessoal algum tipo de **formação geral para a sensibilização**

19% **não informam/formam** os novos efetivos sistematicamente

41% têm **formação específica para a administração**

29% têm **formação obrigatória** para os gestores dos sistemas informáticos que contêm informações sensíveis

55% testaram o pessoal com **simulações de *phishing***

Os controlos essenciais nem sempre são postos em prática ou não são formalizados em normas

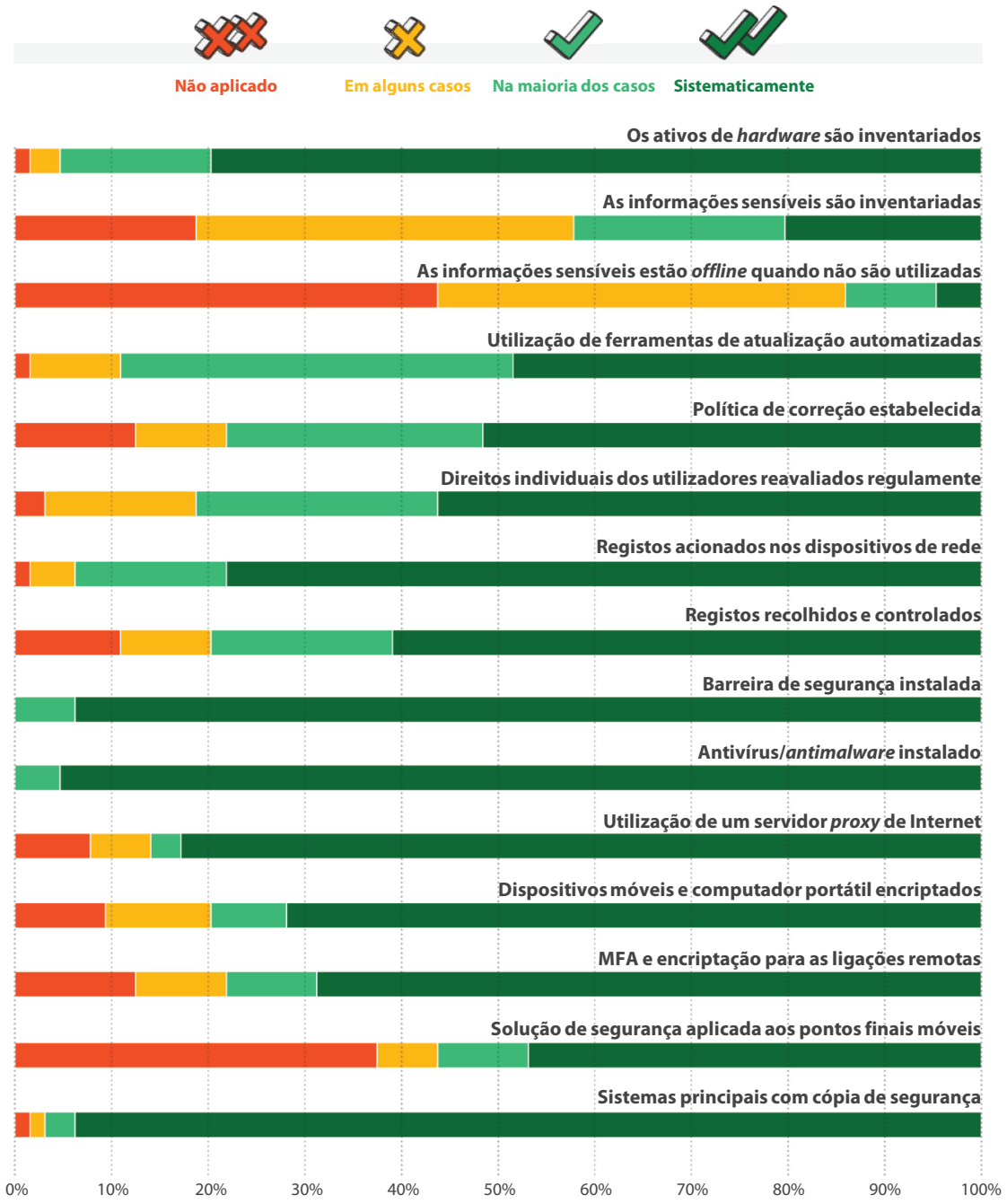
37 O Tribunal solicitou às EUIBA que autoavaliassem a execução de uma seleção de controlos essenciais[22]. Foi selecionado um conjunto de boas práticas que mesmo organizações de menor dimensão poderiam razoavelmente executar[23]. Os resultados

[22] Conjunto de controlos derivados dos CIS Controls 7.1, um quadro de boas práticas supervisionado pelo Centre for Internet Security.

[23] Grupo de implementação 1 (IG1) dos CIS Controls.

são apresentados na ***figura 5***. A maioria das EUIBA inquiridas adotou os controlos essenciais selecionados. No entanto, em algumas áreas, os controlos parecem ser deficientes ou limitados em pelo menos 20% das EUIBA.

Figura 5 – Execução dos controlos essenciais nas EUIBA (resultados da autoavaliação)



Fonte: inquérito do TCE.

38 Para as sete EUIBA incluídas na amostra, o Tribunal solicitou os documentos comprovativos e as normas/políticas correspondentes para cada controlo que declaram ter posto em prática. Obteve estes documentos para 62% dos controlos. Tal

como clarificado durante as entrevistas, em vários casos, os controlos técnicos tinham sido postos em prática, mas não foram formalizados – até à data – em normas ou políticas, o que aumenta o risco de as questões de segurança informática não serem tratadas de forma coerente dentro da mesma EUIBA (ver também o ponto ***24***).

Várias EUIBA não submetem as respetivas disposições em matéria de cibersegurança à prestação regular de uma garantia independente

39 De acordo com a ISACA[24], a auditoria interna é uma das três linhas essenciais de defesa de uma organização, sendo que as outras duas são a gestão e a gestão dos riscos. As auditorias internas contribuem para melhorar a governação da segurança da informação e da segurança informática. O Tribunal examinou a frequência com que as EUIBA recolhem garantias independentes sobre o seu quadro de segurança informática, através de auditorias internas ou externas e de testes proativos das suas ciberdefesas.

40 O Serviço de Auditoria Interna (SAI) da Comissão é responsável, nomeadamente, pela realização de auditorias informáticas à Comissão, às agências descentralizadas, às empresas comuns e ao SEAE. O mandato do serviço abrange 46 (70%) das 65 EUIBA inquiridas e o SAI realizou auditorias relacionadas com a segurança informática em 6 EUIBA diferentes nos últimos cinco anos. Além disso, a DG Recursos Humanos e Segurança é competente para realizar inspeções de segurança informática que abranjam os aspetos técnicos da segurança da informação[25]. Das restantes EUIBA, sete comunicaram ter a sua própria função de auditoria interna que abrange os aspetos informáticos, mas, no caso de doze EUIBA, as respostas ao inquérito do Tribunal não foram suficientes para determinar se dispõem de tal capacidade de auditoria interna.

41 As auditorias de segurança informática externas realizadas por entidades independentes são outra forma de obter uma garantia independente. Apesar da rápida evolução do panorama cibernético, entre o início de 2015 e o primeiro trimestre de 2021, 34% das EUIBA não tinham sido objeto de qualquer auditoria de segurança informática interna ou externa. Uma desagregação do último número por tipo de EUIBA revela que 75% dos organismos, 66% das empresas comuns e 45% das

[24] ISACA, *Auditing Cyber Security: Evaluating Risk and Auditing Controls*, 2017.

[25] Decisão 46/2017 relativa à segurança dos sistemas de comunicação e informação da Comissão Europeia.

missões civis da UE não foram objeto de uma auditoria de segurança informática interna ou externa desde 2015.

42 Além das auditorias internas e externas, outra forma de as organizações obterem garantias sobre o seu quadro de segurança informática consiste em testar proativamente as suas ciberdefesas para detetar vulnerabilidades. Os testes de penetração (também conhecidos como pirataria informática ética), que consistem em ciberataques simulados autorizados em sistemas informáticos individuais, são um dos métodos para o fazer. Em resposta ao inquérito do Tribunal, 69% das EUIBA declararam ter realizado pelo menos um teste de penetração nos últimos cinco anos. Em 45% dos casos, a CERT-UE foi a entidade que realizou os testes de penetração.

43 Os exercícios de "equipa de segurança ofensiva" são outra forma de testar as ciberdefesas através de ataques simulados, recorrendo a técnicas recentemente utilizadas em ataques reais. São mais complexos e abrangentes do que os testes de penetração, na medida em que envolvem múltiplos sistemas e potenciais vias de ataque. As EUIBA realizam-nos com menor frequência: 46% das EUIBA comunicaram pelo menos um exercício de equipa de segurança ofensiva nos últimos cinco anos. A CERT-UE realizou 75% destes exercícios. Os exercícios de equipa de segurança ofensiva exigem uma quantidade substancial de trabalho de preparação e execução e a CERT-UE tem, atualmente, capacidade para realizar um máximo de cinco a seis exercícios por ano.

44 Excluindo duas EUIBA criadas recentemente, 16 (25%) das EUIBA inquiridas não tinham realizado testes de penetração nem exercícios de equipa de segurança ofensiva nos últimos cinco anos. De um modo geral, sete EUIBA (10%) não foram objeto de qualquer forma de garantia independente sobre as suas disposições em matéria de segurança informática: uma empresa comum, uma agência descentralizada e cinco missões civis.

PRINCIPAIS VALORES: **Garantia independente sobre a segurança informática nas EUIBA nos últimos cinco anos**

66%
das EUIBA foram **sujeitas** a, pelo menos, **uma auditoria interna ou externa** relacionada com a segurança informática

69%
realizaram, pelo menos, **um teste de penetração**

46%
realizaram, pelo menos, **um exercício de equipa de segurança ofensiva**

10%
não foram sujeitas a qualquer forma de **auditoria ou teste independente** de segurança informática

As EUIBA estabeleceram mecanismos para a cooperação, mas existem insuficiências

45 A presente secção analisa os intervenientes e os comités criados para promover a cooperação entre as EUIBA na área da cibersegurança, assim como a governação interinstitucional e as disposições de coordenação. Mais especificamente, o Tribunal examinou dois intervenientes interinstitucionais, a ENISA e a CERT-UE, e dois comités interinstitucionais, o Comité Interinstitucional para a Transformação Digital (ICDT), em particular o subgrupo de cibersegurança (CSSG), e o Comité Consultivo para as Tecnologias da Informação e da Comunicação (ICTAC). O Tribunal avaliou igualmente em que medida proporcionaram sinergias para aumentar a preparação para a cibersegurança por parte das EUIBA.

Existe uma estrutura formalizada para as EUIBA coordenarem as suas atividades, embora haja problemas relacionados com a governação

46 O ICDT e o ICTAC são os dois principais comités que promovem a cooperação em matéria de TI entre as EUIBA. Composto pelos gestores informáticos das instituições e organismos da UE, o ICDT é um fórum para promover o intercâmbio de informações e a cooperação. Tem um subgrupo de cibersegurança (o CSSG do ICDT) que responde perante o ICDT e pode recomendar a tomada de decisões sobre questões específicas. O ICTAC, por sua vez, é um subgrupo da Rede de Agências da UE (EUAN), uma rede informal criada pelos chefes das agências da UE que se centra na cooperação entre agências e empresas comuns. Tanto o ICDT como o ICTAC têm funções claramente definidas e complementares: o ICTAC abrange as agências descentralizadas e as empresas comuns, enquanto o ICDT abrange instituições e organismos. Por natureza, o ICDT e o ICTAC são grupos consultivos e fóruns bastante informais para o intercâmbio de informações e de boas práticas. São apresentadas mais informações sobre estes comités interinstitucionais no ***anexo II***.

A representação das EUIBA nos fóruns relevantes nem sempre é adequada

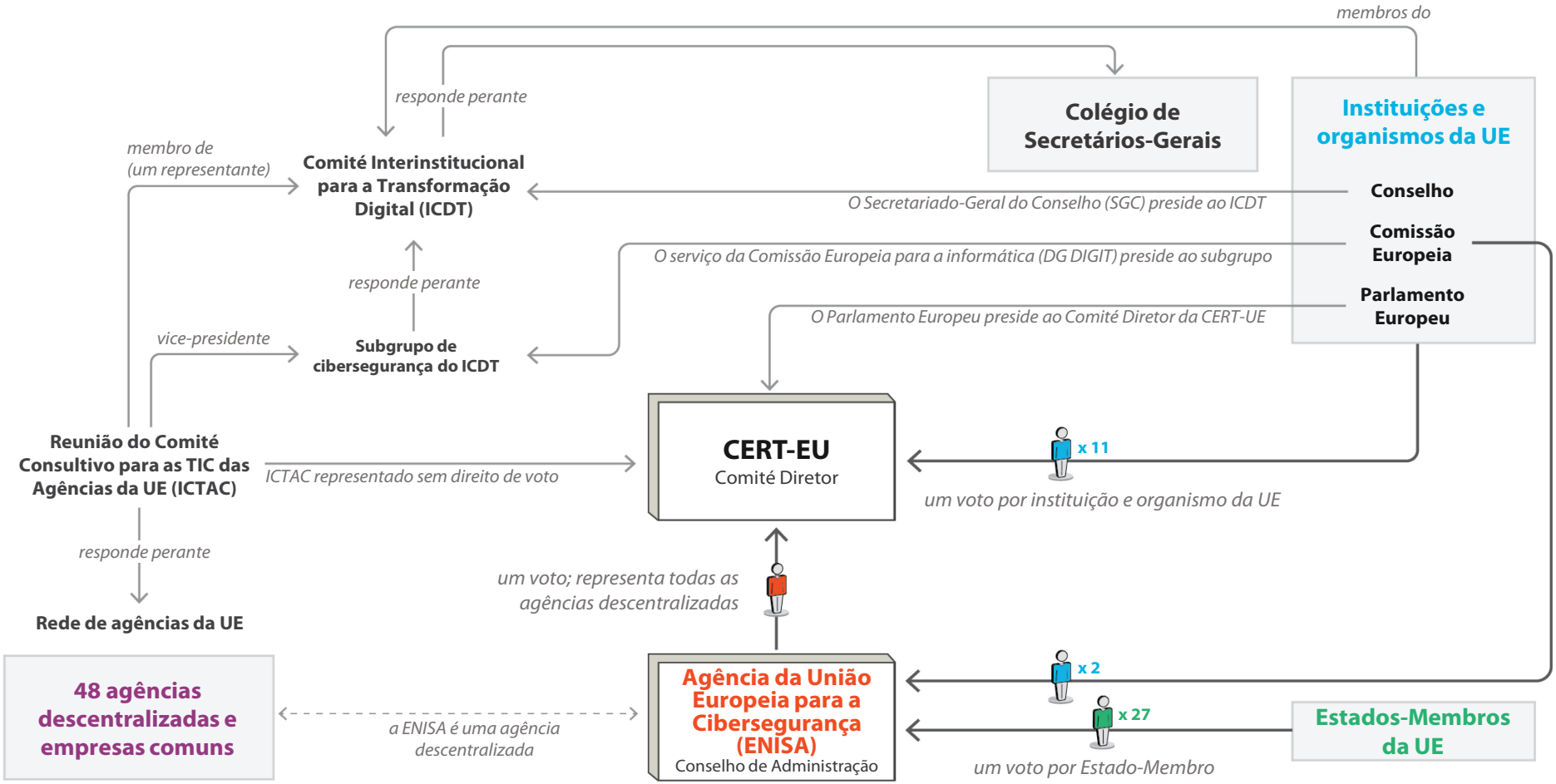
47 Embora as estruturas de representação sejam claras, nem todas as EUIBA consideram suficiente a sua representação efetiva. Quando lhes foi solicitado, no inquérito do Tribunal, que opinassem sobre se as suas necessidades eram tidas em conta de forma suficiente nos fóruns interinstitucionais pertinentes e se a sua representação nos conselhos decisores era adequada, 42% das EUIBA discordaram. Algumas das que têm menor dimensão consideraram que não têm recursos suficientes para participar ativamente nos fóruns interinstitucionais.

48 O comité diretor da CERT-UE, seu principal órgão decisório, também não é representativo, no conjunto, das suas "partes". A CERT-UE presta serviços a 87 EUIBA e a três organizações que não o são. No entanto, o seu comité diretor inclui apenas representantes dos 11 signatários do acordo interinstitucional (as sete instituições da EU, em conjunto com o SEAE, o Comité Económico e Social, o Comité das Regiões Europeu e o Banco Europeu de Investimento) e um representante da ENISA, dispondo cada um deles de um voto[26].

49 Mais de metade das "partes" da CERT-UE são agências descentralizadas da UE e empresas comuns, que têm em conjunto cerca de 12 000 efetivos. Formalmente, os seus interesses são representados no comité diretor da CERT-UE pela ENISA. No entanto, o mandato da ENISA para representar as agências da UE e as empresas comuns é fraco, uma vez que esta agência não foi diretamente nomeada ou eleita pelas mesmas. Na prática, os pontos de vista das agências descentralizadas e das empresas comuns são expressos nas reuniões do comité diretor por um representante do ICTAC, que está autorizado a participar nas mesmas para auxiliar a ENISA no seu papel de representante das agências. Apesar de expressar os pontos de vista e os interesses de 48 EUIBA, o representante do ICTAC não tem atualmente qualquer lugar formal ou direito de voto no comité diretor. Em abril de 2021, o ICTAC enviou ao presidente do comité diretor da CERT-UE um pedido formal de direito de voto no conselho executivo. À data da redação do presente documento, este pedido ainda não foi deferido. A ***figura 6*** apresenta uma visão global da representação das EUIBA nos comités e conselhos decisores.

[26] Artigo 7º do Acordo Interinstitucional (AII), assinado em 20.12.2017.

Figura 6 – Visão global da governação e da representação em matéria de cibersegurança nos comités e conselhos decisores



Fonte: TCE.

50 A governação interinstitucional em matéria de cibersegurança das EUIBA é fragmentada e nenhuma entidade dispõe atualmente de uma visão global abrangente da maturidade em termos de cibersegurança das EUIBA, nem da autoridade para assumir um papel de liderança ou aplicar regras vinculativas comuns. Tanto a ENISA como a CERT-UE só podem "apoiar" e "auxiliar" as EUIBA. Os comités pertinentes não têm poder decisório e apenas podem formular recomendações às EUIBA. Além disso, para um quinto das EUIBA inquiridas, também não é evidente a quem devem recorrer para obter um serviço, ferramenta ou solução específicos.

Existem memorandos de entendimento entre os principais intervenientes, mas, até à data, ainda não produziram resultados concretos

51 Em maio de 2018, foi assinado um memorando de entendimento entre a ENISA, a CERT-UE, o Centro Europeu da Cibercriminalidade (EC3) da Europol e a Agência Europeia de Defesa (AED). O documento centrou-se em cinco áreas de cooperação: intercâmbio de informações, educação e formação, exercícios de cibersegurança, cooperação técnica e questões estratégicas e administrativas. Embora este memorando de entendimento possa ajudar a evitar duplicações por dispor de um programa de trabalho comum, o Tribunal não encontrou provas de que tenha produzido resultados concretos e ações conjuntas.

52 O Regulamento Cibersegurança, que entrou em vigor em junho de 2019, previa a assinatura de um novo convénio de cooperação específico entre a CERT-UE e a ENISA. É de salientar que foi necessário mais de um ano e meio para, finalmente, se assinar o memorando de entendimento, em fevereiro de 2021. Este memorando de entendimento tenta estabelecer uma cooperação estruturada entre a CERT-UE e a ENISA. Define as suas áreas de cooperação (desenvolvimento de capacidades, cooperação operacional e conhecimento e informação) e estabelece uma divisão aproximada de funções entre ambas: a CERT-UE assumirá a liderança na prestação de assistência às EUIBA e a ENISA contribuirá para esse esforço. O memorando de entendimento não define as disposições práticas, uma vez que estas são especificadas num plano de cooperação anual. O primeiro plano de cooperação anual para 2021 foi adotado pelo conselho de administração da ENISA em julho de 2021 e pelo comité diretor da CERT-UE em setembro de 2021. Por conseguinte, é demasiado cedo para a auditoria do Tribunal avaliar se este plano produziu quaisquer resultados tangíveis.

53 Uma vez que ambos os memorandos de entendimento referidos nos pontos ***51*** e ***52*** têm objetivos e áreas de cooperação comuns, como a formação, os exercícios ou o intercâmbio de informações, existe um risco de sobreposições e redundâncias.

As potenciais sinergias através da cooperação ainda não são plenamente exploradas

Foram tomadas medidas positivas para alcançar sinergias

54 Os programas de trabalho dos comités ICTAC e CSSG do ICDT identificam tópicos pertinentes em que é possível obter ganhos de eficiência através da colaboração. Os exemplos práticos de iniciativas que permitiram que as EUIBA beneficiassem das sinergias incluem:

- acordos-quadro interinstitucionais;
- um centro comum de recuperação em caso de catástrofe, disponibilizado desde 2019 pelo Instituto da Propriedade Intelectual da União Europeia (EUIPO) para as agências descentralizadas, permitindo uma redução de custos de, pelo menos, 20% em comparação com os preços de mercado (nove agências adotaram esta solução de recuperação em caso de catástrofe);
- acordos entre seis empresas comuns situadas no mesmo edifício para partilhar infraestruturas comuns e um quadro comum de segurança informática (desde 2014).

55 Outro exemplo importante é o "GovSec", um sistema que ajuda as EUIBA a realizar avaliações de riscos com vista à adoção de soluções em nuvem. De acordo com o inquérito do Tribunal, 7% das EUIBA já utilizam algumas plataformas em nuvem públicas e várias das que não o fazem tencionam migrar para a nuvem. Desde 2019, a Comissão adotou uma abordagem "*cloud first*", com vista a uma oferta de serviços segura, híbrida e multinuvem[27]. A Comissão atua igualmente como corretor de computação em nuvem para todas as EUIBA, no contexto do acordo-quadro "*Cloud II*". Gerir os riscos de segurança e de proteção de dados em plataformas em nuvem exige novas competências e uma abordagem diferente, em comparação com as infraestruturas informáticas tradicionais situadas nas instalações. A gestão eficaz dos riscos de segurança da informação na nuvem é um desafio comum para as EUIBA e o GovSec é um exemplo de uma solução que pode responder às necessidades de várias, se não de todas, as EUIBA.

[27] Comissão Europeia, *The European Commission Cloud Strategy*, 2019.

A colaboração e a partilha de práticas entre EUIBA ainda não são ideais

56 A existência de comités interinstitucionais não origina automaticamente sinergias e as EUIBA nem sempre partilham as boas práticas, o saber-fazer, as metodologias e os ensinamentos retirados. Além disso, cabe a cada EUIBA decidir qual o seu nível de participação no CSSG do ICDT. Os membros deste subgrupo, apesar de participarem nas reuniões, apenas podem contribuir na medida em que as suas funções habituais nas EUIBA o permitam, o que já abrandou o progresso da execução das ações acordadas por alguns grupos de trabalho.

57 O Tribunal detetou áreas específicas em que não existem convénios para que as EUIBA partilhem experiências e iniciativas. Por exemplo, no âmbito do acordo-quadro "*Network Defence Capability*" (NDC), as EUIBA podem solicitar um estudo para consolidar os requisitos de cibersegurança e encontrar soluções. Todavia, não existe um repositório dos estudos realizados ou solicitados por outras EUIBA, pelo que estas podem solicitar o mesmo estudo várias vezes. Além disso, as EUIBA não divulgam sistematicamente entre si que têm relações contratuais com fornecedores específicos ou que utilizam uma solução de *software* específica. Esta lacuna de conhecimentos pode resultar em custos adicionais e na perda de sinergias.

58 As EUIBA também não partilham sistematicamente entre si informações sobre projetos de cibersegurança que estão a realizar, mesmo que estes possam ter um impacto interinstitucional. O mandato do CSSG do ICDT inclui uma disposição no sentido de as EUIBA partilharem informações sobre novos projetos suscetíveis de afetar a cibersegurança de outras EUIBA e/ou a proteção de informações delas provenientes. No entanto, o CSSG do ICDT não é mantido ao corrente de tais projetos.

59 Quando uma nova agência é criada, tem de construir a partir do zero a sua infraestrutura informática e o seu quadro de segurança informática. Não existe um "catálogo de serviços", uma caixa de ferramentas ou orientações/requisitos claros para as novas agências. O resultado é uma heterogeneidade substancial dos ambientes informáticos no conjunto das EUIBA, uma vez que cada organização é potencialmente livre de adquirir os seus próprios serviços, infraestruturas, *software* e equipamento informático. O mesmo acontece com o quadro de segurança informática, na ausência de requisitos e normas comuns. Esta situação provoca uma potencial duplicação de esforços e uma utilização ineficiente dos fundos da UE, mas também uma maior complexidade para a CERT-UE em termos do apoio que deve fornecer.

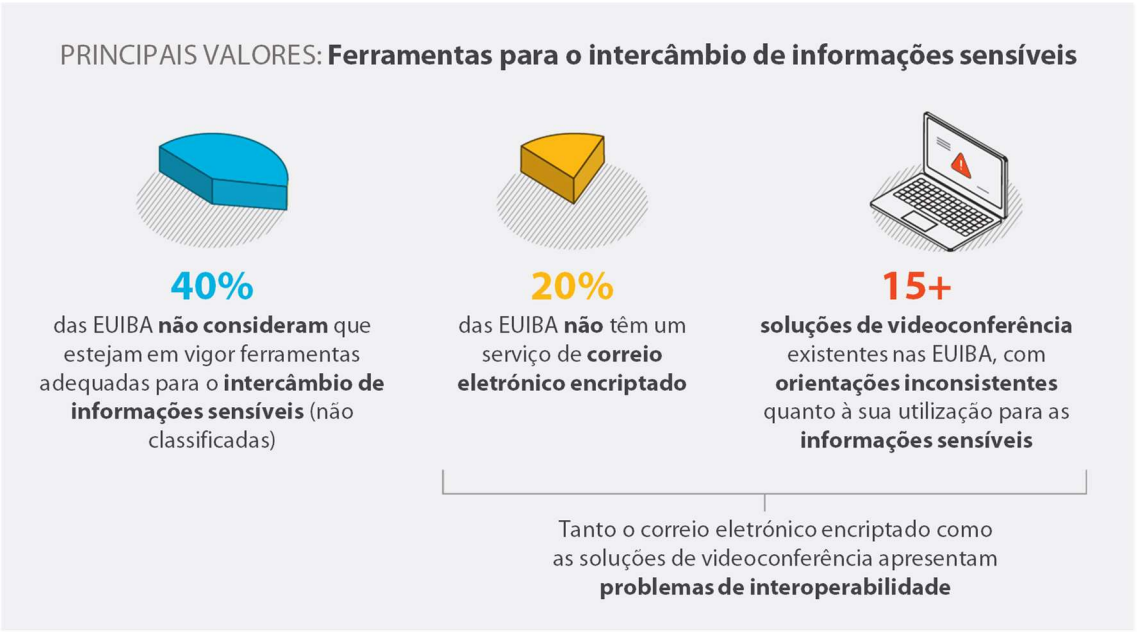
Existem insuficiências práticas no intercâmbio de informação sensível

60 Algumas EUIBA ainda não dispõem de soluções adequadas para o intercâmbio de informações sensíveis não classificadas. Aquelas que dispõem destas soluções, de um modo geral, adotaram os seus próprios produtos e sistemas diferentes, o que significa que a interoperabilidade é uma questão problemática. As plataformas seguras comuns existem apenas para fins específicos, por exemplo, as plataformas que a CERT-UE disponibiliza a todas as "partes" para o intercâmbio de informações sensíveis sobre incidentes, ameaças e vulnerabilidades.

61 Por exemplo, mais de 20% das EUIBA não dispõem de um serviço de correio eletrónico encriptado. Aquelas que dispõem desse serviço enfrentam frequentemente problemas de interoperabilidade e os certificados não são mutuamente reconhecidos. O ICTAC e o ICDT têm vindo a debater opções com vista a uma solução escalável e interoperável há anos e, em 2018, foi realizado um projeto-piloto. No entanto, esta questão ainda não foi resolvida.

62 Outra questão é a ausência de marcações comuns para informações sensíveis não classificadas. As marcações são categorizações que indicam aos detentores de informações os requisitos específicos de proteção dessas informações. Diferem entre as EUIBA, o que dificulta o intercâmbio e o tratamento adequado das informações.

63 Em 2020, a pandemia de COVID-19 obrigou as EUIBA a adotarem ferramentas de comunicação e videoconferência em grande escala, a fim de assegurar a continuidade das atividades. O Tribunal identificou, pelo menos, 15 soluções de *software* de videoconferência diferentes utilizadas pelas EUIBA. Mesmo quando distintas EUIBA utilizam a mesma solução/plataforma, a interoperabilidade continua muitas vezes a ser insuficiente, ainda que todas as partes utilizem a mesma solução de *software*. Além disso, as orientações sobre as informações (em termos de sensibilidade) que poderiam ser partilhadas ou discutidas numa determinada plataforma divergiam entre as EUIBA. Estas questões provocam ineficiências económicas e operacionais e podem criar problemas de segurança.



A ENISA e a CERT-UE ainda não prestaram às EUIBA todo o apoio de que estas necessitam

64 Na presente secção, o Tribunal examina as duas principais entidades encarregadas de apoiar as EUIBA no domínio da cibersegurança: a ENISA e a CERT-UE, avaliando se o apoio prestado por ambas chegou às EUIBA e está a dar resposta às suas necessidades e destacando as razões subjacentes às insuficiências assinaladas.

A ENISA é um interveniente fundamental no panorama da cibersegurança da UE, mas o seu apoio, até à data, chegou a muito poucas EUIBA

65 Em junho de 2019, entrou em vigor o Regulamento Cibersegurança[28], que veio substituir a anterior base jurídica da ENISA[29] e conferiu à agência um mandato mais robusto. Mais especificamente, prevê que a ENISA deve apoiar ativamente os Estados-Membros e as EUIBA na melhoria da cibersegurança através do desenvolvimento de capacidades, do reforço da cooperação operacional e do estabelecimento de sinergias. Na área do desenvolvimento de capacidades, a ENISA tem agora um mandato para prestar assistência às EUIBA "nos seus esforços para

[28] As tarefas da ENISA estão enumeradas no capítulo II (artigos 5º a 12º) do Regulamento (UE) 2019/881.

[29] Regulamento (UE) nº 526/2013 do Parlamento Europeu e do Conselho; relativamente às tarefas da ENISA ao abrigo deste regulamento, ver o artigo 3º.

melhorar a prevenção, deteção e análise de ciberameaças e incidentes, em especial através de um apoio adequado à CERT-UE"[30]. A ENISA deve igualmente prestar assistência às instituições da UE no desenvolvimento e na revisão das estratégias da União Europeia em matéria de cibersegurança, promovendo a sua divulgação e acompanhando os progressos realizados na sua execução.

66 Embora o Regulamento Cibersegurança indique claramente que a ENISA deve apoiar as EUIBA na melhoria da sua cibersegurança, esta agência ainda não concluiu quaisquer planos de ação relativamente ao seu objetivo de apoio ao reforço das capacidades das EUIBA (ver ***caixa 3*** para mais pormenores).

[30] Artigo 6º do Regulamento (UE) 2019/881.

Caixa 3

Alinhamento insuficiente entre os objetivos e as realizações da ENISA em relação às EUIBA

Estas são algumas das prioridades trienais da ENISA enumeradas no programa de trabalho plurianual para o período de 2018-2020, no âmbito do objetivo 3.2 "Apoiar o desenvolvimento de capacidades das instituições da UE":

- prestar aconselhamento proativo às instituições da UE sobre o reforço da sua segurança das redes e da informação (SRI) (identificar as prioridades para as agências e organismos da UE com maiores necessidades em termos de desenvolvimento de capacidades em matéria de segurança das redes e da informação, estabelecendo interações regulares com as mesmas (por exemplo, oficinas anuais) e centrar-se nestas prioridades);

- procurar apoiar e ajudar as instituições da UE em relação às abordagens em matéria de segurança das redes e da informação (criar parcerias com a CERT-UE e instituições com capacidades fortes em matéria de seguranças das redes e da informação, com vista a apoiar as suas ações no âmbito deste objetivo.)

Nos programas de trabalho da ENISA para 2018, 2019 e 2020, existem apenas dois objetivos operacionais (realizações) no âmbito do objetivo 3.2:

- "Participação no Comité Diretor da CERT-UE e representação das agências da UE utilizando o serviço CERT-UE".

- "Cooperação com os organismos pertinentes da UE em iniciativas que abranjam a dimensão de segurança das redes e da informação relacionada com as suas missões (incluindo a AESA, CERT-UE, Agência Europeia de Defesa, EC3)".

Os objetivos operacionais não incluem qualquer atividade relacionada com o aconselhamento proativo. Além disso, o objetivo de identificar prioridades para as agências com maiores necessidades não se traduziu em realizações operacionais, uma vez que foi substituído pelo objetivo de estabelecer contactos com as agências para representar as suas necessidades no comité diretor da CERT-UE.

67 O principal órgão de decisão da ENISA é o seu conselho de administração, composto por um membro nomeado por cada um dos 27 Estados-Membros e dois membros nomeados pela Comissão[31] (ver ***figura 6***). Cada membro dispõe de um voto e as decisões são tomadas por maioria[32]. Consequentemente, as ações relativas aos Estados-Membros podem ter maior prioridade em relação às ações relativas às EUIBA. Por exemplo, no programa de trabalho da ENISA para 2018, o conselho de administração decidiu, por falta de recursos suficientes, dar prioridade a determinadas atividades e eliminar três, uma das quais era "apoiar a avaliação das políticas/procedimentos/práticas existentes em matéria de segurança das redes e da informação nas instituições da UE". Esta atividade destinava-se a permitir à ENISA formar uma visão global das práticas das EUIBA e da maturidade indicativa em matéria de cibersegurança, como base para futuras ações específicas.

68 Por conseguinte, a ambição da ENISA de prestar assistência proativa às EUIBA, expressa nos seus objetivos estratégicos, não se concretizou em objetivos operacionais nem em ações concretas. Até à data, o apoio nas áreas de desenvolvimento de capacidades e cooperação operacional tem-se limitado a algumas EUIBA em específico, mediante pedido.

69 O Regulamento Cibersegurança estipula igualmente que, a fim de apoiar as EUIBA no desenvolvimento de capacidades, a ENISA deve prestar o apoio adequado à CERT-UE. À data da auditoria, este apoio tinha-se limitado a algumas ações específicas. Por exemplo, em 2019, a ENISA realizou um exame pelos pares da CERT-UE, no contexto da sua filiação na rede da CSIRT da UE (criada pela Diretiva SRI).

70 De acordo com as respostas ao inquérito do Tribunal, a ENISA publica relatórios e orientações de elevada qualidade sobre cibersegurança, alguns dos quais são utilizados pelas EUIBA. No entanto, não existem orientações específicas que visem as EUIBA e o seu próprio ambiente e necessidades. As EUIBA, especialmente as menos avançadas no domínio da cibersegurança, necessitam de orientações práticas não só sobre "o que" fazer, mas também sobre "como" fazê-lo. Até à data, a ENISA e a CERT-UE prestaram pouco apoio deste tipo e fizeram-no de forma não sistemática.

---

[31] Artigo 14º do Regulamento Cibersegurança.

[32] Artigo 18º do Regulamento Cibersegurança.

71 A ENISA organizou uma série de ações de formação sobre cibersegurança, dirigidas principalmente às autoridades dos Estados-Membros, mas que acolheram também um pequeno número de participantes provenientes de EUIBA. Ofereceu apenas duas formações de autoaprendizagem dirigidas especificamente às EUIBA. Disponibiliza igualmente material de formação em linha no seu sítio Web, ao qual as EUIBA podem aceder. Contudo, até à data, estas ações de formação têm-se destinado sobretudo a especialistas técnicos da CSIRT e, como tal, não são úteis para a maioria das EUIBA.

72 Além da formação, a ENISA pode apoiar as EUIBA através de exercícios de cibersegurança. Em outubro de 2020, em colaboração com a CERT-UE, a ENISA ajudou a realizar um exercício de cibersegurança para o ICTAC, o único exercício que organizou especificamente para participantes das EUIBA. Além disso, ajudou a organizar uma série de exercícios a pedido de algumas EUIBA (por exemplo, a eu-LISA, a EMSA, o Parlamento Europeu e a Europol), principalmente para as suas partes interessadas nas autoridades dos Estados-Membros, com a participação de alguns efetivos das EUIBA.

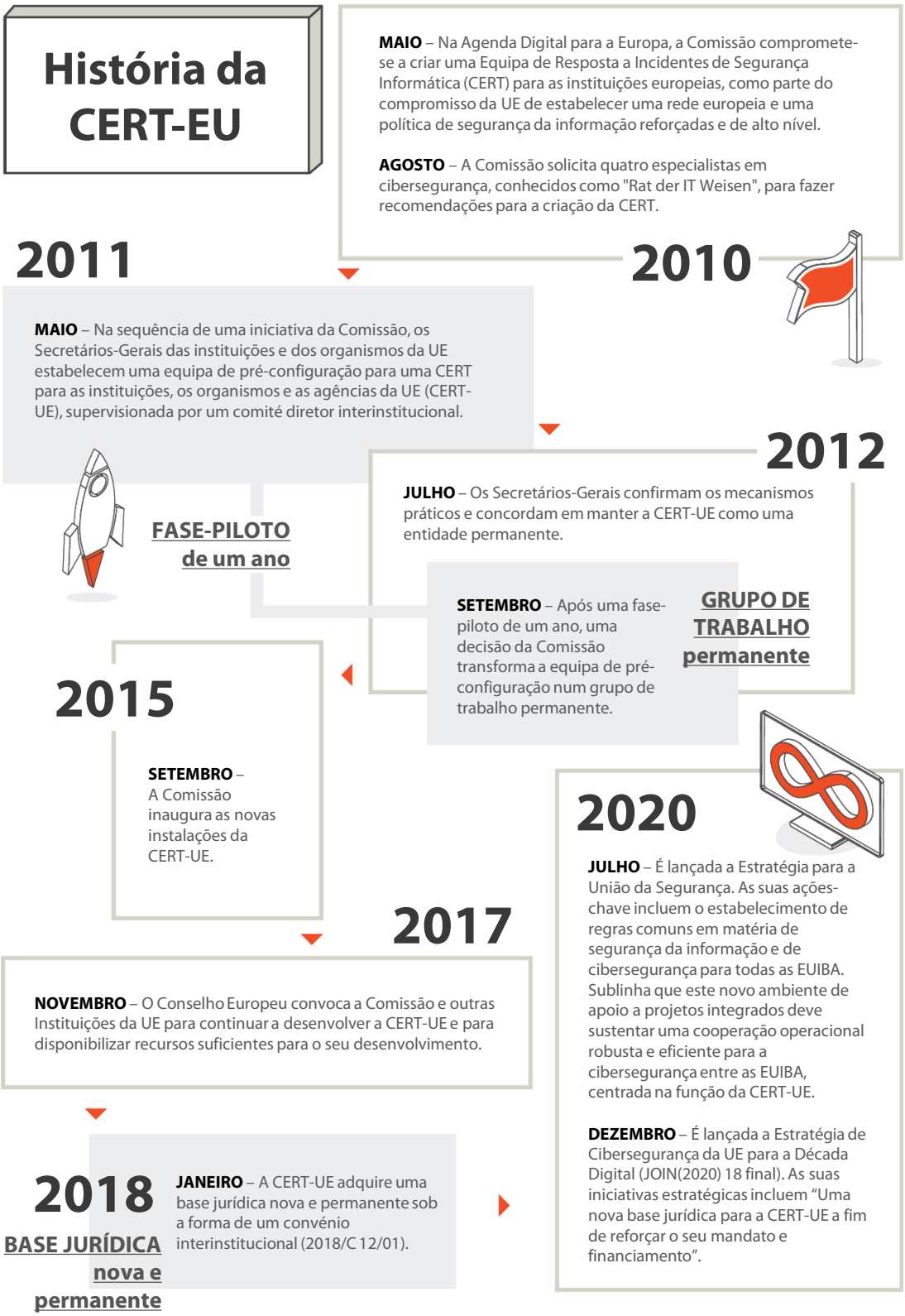
73 O Regulamento Cibersegurança também introduziu uma nova função para a ENISA, que passou a dever prestar assistência às EUIBA a respeito das suas políticas de divulgação das vulnerabilidades numa base voluntária. No entanto, a ENISA ainda não tem uma visão global das políticas individuais de revelação de vulnerabilidades das EUIBA e não as ajuda a definir e a aplicar estas políticas.

A CERT-UE é muito valorizada pelas suas "partes", mas não dispõe de meios proporcionais aos desafios atuais em matéria de cibersegurança

74 Na sequência de uma série de iniciativas (ver ***figura 7***), em setembro de 2012 uma decisão da Comissão[33] criou a Equipa de Resposta a Emergências Informáticas para as instituições e agências da UE (CERT-UE) como um grupo de trabalho permanente para as EUIBA (ver ponto ***08***).

[33] Comunicado de imprensa da Comissão Europeia: "Cibersegurança reforçada nas instituições europeias após o sucesso de um projeto-piloto".

Figura 7 – História da CERT-UE



Fonte: TCE.

75 Embora seja independente nas suas operações, a CERT-UE continua a ser um grupo de trabalho, sem personalidade jurídica. A nível administrativo, está situada na Comissão Europeia (DG DIGIT), da qual recebe apoio logístico e administrativo. O objetivo da CERT-UE é tornar mais seguras as infraestruturas de TIC das EUIBA através do reforço da sua capacidade de lidar com ciberameaças e vulnerabilidades e de prevenir, detetar e responder a ciberataques. A CERT-UE tem cerca de 40 efetivos, organizados em equipas de especialistas centradas, por exemplo, na informação sobre ameaças, na peritagem forense digital e na resposta a incidentes.

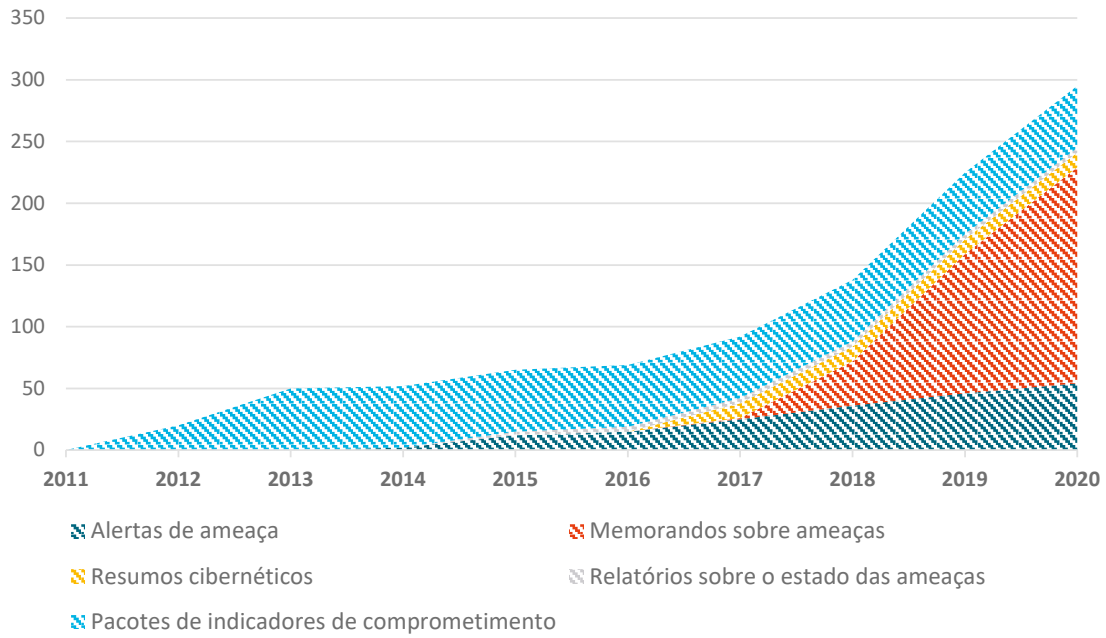
A CERT-UE é um parceiro apreciado, com uma crescente carga de trabalho

76 A CERT-UE solicita *feedback* e sugestões aos seus constituintes através de oficinas trimestrais e reuniões bilaterais anuais, bem como de inquéritos de satisfação. De acordo com os inquéritos de satisfação e o inquérito do Tribunal, os constituintes estão particularmente satisfeitos com os serviços prestados pela CERT-UE. A evolução do catálogo de serviços da CERT-UE atesta o seu esforço de adaptação às necessidades das EUIBA.

77 Embora as EUIBA de grande dimensão com capacidade interna significativa tendam a utilizar a CERT-UE principalmente como plataforma de partilha de informações e fonte de informações sobre ameaças, as EUIBA de menor dimensão dependem da CERT-UE para uma gama mais vasta de serviços, como acompanhamento de registos, testes de penetração, exercícios de equipa de segurança ofensiva e apoio à resposta a incidentes. Os serviços da CERT-UE são particularmente valiosos para as EUIBA de menor dimensão, devido ao saber-fazer interno limitado e à falta de economias de escala das mesmas (ver pontos ***31*** e ***33***).

78 A CERT-UE reforçou as suas capacidades e procedimentos nos últimos anos, num contexto de aumento dramático das ameaças e dos incidentes. O número de produtos de informação da CERT-UE, em especial os alertas e memorandos de ameaça, tem vindo a crescer constantemente (***figura 8***). Em 2020, a CERT-UE emitiu 171 memorandos de ameaça e 53 alertas de ameaça (números consideravelmente superiores aos 80 memorandos e 40 alertas que inicialmente esperava emitir).

Figura 8 – Aumento dos produtos de informação sobre ameaças



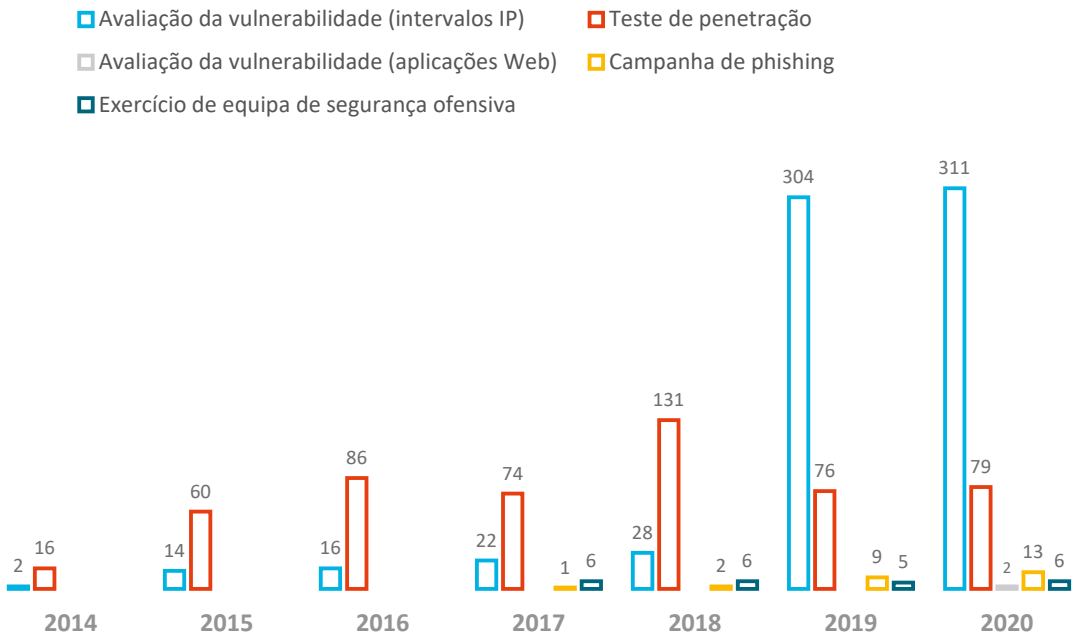
Fonte: TCE, com base em dados da CERT-UE.

79 A CERT-UE também apoia as EUIBA no tratamento de ciberincidentes. Enquanto 52% das EUIBA dispõem de uma equipa de resposta interna ou, pelo menos, de um coordenador de incidentes, os restantes 48% dependem da CERT-UE e/ou de outros prestadores externos em caso de incidente. No entanto, mesmo as EUIBA de grande dimensão com capacidade de resposta interna podem solicitar o apoio da CERT-UE para lidar com incidentes complexos.

80 O número total de incidentes tratados pela CERT-UE aumentou de 561 em 2019 para 884 em 2020. Os incidentes significativos, em particular, aumentaram de apenas 1 em 2018 para 13 em 2020. Em 2021, o número de incidentes significativos atingiu os 17, uma subida em relação aos 13 verificados em 2020, que, por sua vez, foi um ano recorde. Geralmente, estes incidentes significativos são causados por ameaças altamente sofisticadas. Podem afetar várias EUIBA, envolver contactos com as autoridades e, normalmente, implicam semanas ou meses de trabalho para as entidades em causa e para que a CERT-UE os consiga investigar e erradicar.

81 A CERT-UE é também o principal fornecedor de avaliações e testes proativos das ciberdefesas das EUIBA. Na ***figura 9*** é apresentado um sumário da atividade da CERT-UE nesta área. Além disso, desde 2020, a CERT-UE também efetua análises externas de rede.

Figura 9 – Testes e avaliações realizados pela CERT-UE



Fonte: TCE, com base em dados da CERT-UE.

Os constituintes não partilham as informações pertinentes com a CERT-UE em tempo útil

82 O Acordo Interinstitucional[34] estabelece que os constituintes devem notificar a CERT-UE de ciberincidentes significativos. No entanto, na prática, tal nem sempre aconteceu. O Acordo Interinstitucional não prevê um mecanismo para impor a comunicação obrigatória e atempada de incidentes "significativos" por parte dos constituintes da CERT-UE. A definição genérica de "acidentes significativos" constante do Acordo Interinstitucional deixa ao critério das EUIBA a comunicação de um incidente. De acordo com a gestão da CERT-UE, alguns constituintes não partilharam informações sobre incidentes significativos em tempo útil, o que dificulta a função da CERT-UE enquanto plataforma de intercâmbio de informações em matéria de cibersegurança e de coordenação da resposta a incidentes para todas as EUIBA. Por exemplo, um constituinte que foi confrontado com uma ameaça muito sofisticada não informou a CERT-UE nem solicitou o seu apoio. Esta situação impediu a CERT-UE de obter informações sobre ciberameaças que teriam sido úteis para apoiar outros constituintes que enfrentavam a mesma ameaça. Pelo menos seis EUIBA foram afetadas por este ataque.

[34] Artigo 3, nº 3, do Acordo Interinstitucional (AII), assinado em 20.12.2017.

83 Os constituintes também não partilharam ativamente informações em tempo útil com a CERT-UE sobre ciberameaças e vulnerabilidades que os afetam, apesar de o Acordo Interinstitucional[35] solicitar que o façam. A equipa da CERT-UE dedicada à peritagem forense digital e à resposta a incidentes não recebeu notificações de vulnerabilidades ou deficiências nos controlos detetadas fora do contexto de incidentes que está a investigar ativamente. As "partes" não partilham proativamente as conclusões pertinentes das auditorias de segurança internas ou externas.

84 Além disso, o Acordo Interinstitucional não obriga as EUIBA a comunicar à CERT-UE alterações significativas no seu ambiente informático, pelo que as "partes" não informaram sistematicamente a CERT-UE das alterações pertinentes. Por exemplo, as EUIBA nem sempre informam a CERT-UE de quaisquer alterações nos seus intervalos IP (ou seja, a lista de endereços Internet da sua infraestrutura). A CERT-UE necessita de intervalos IP atualizados para, por exemplo, efetuar análises quando são detetadas vulnerabilidades importantes. O facto de as EUIBA não informarem a CERT-UE de tais alterações afeta a capacidade de a CERT-UE as apoiar. A não comunicação à CERT-UE prejudica também a sua capacidade de acompanhar os sistemas e resulta em trabalho acrescido para corrigir dados incorretos nas ferramentas de acompanhamento. De acordo com a sua administração, por vezes a CERT-UE descobre infraestruturas informáticas anteriormente desconhecidas quando está a lidar com um incidente. Acresce que, para além de casos específicos, a CERT-UE não dispõe atualmente de uma visão global abrangente dos sistemas e redes informáticos do conjunto das EUIBA.

85 Na ausência de qualquer mecanismo de aplicação no Acordo Interinstitucional, a comunicação de informações pelas EUIBA à CERT-UE continuará a não ser sistemática, apesar de se tratar de um elemento essencial para que esta desempenhe um papel central na preparação das EUIBA em matéria de cibersegurança.

[35] Artigo 3º, nº 2, do Acordo Interinstitucional (AII).

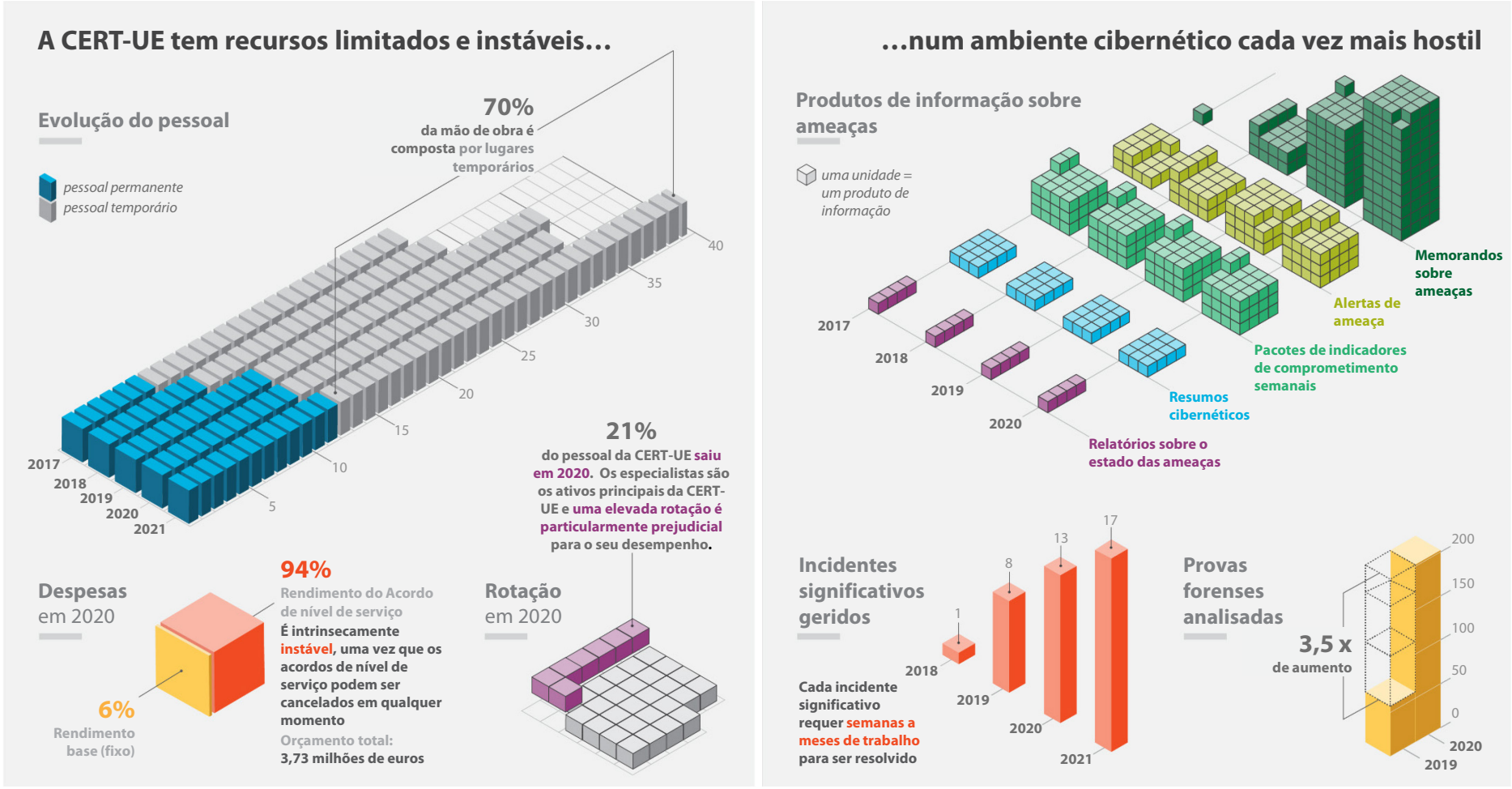
Os recursos da CERT-UE são instáveis, não sendo proporcionais ao nível de ameaça atual

86 O Acordo Interinstitucional[36] estabelece que "a CERT-UE deve ser dotada de financiamento e recursos humanos sustentáveis, ficando garantida uma boa relação custo-benefício, bem como de um núcleo adequado de pessoal permanente". O ativo mais importante da CERT-UE é o seu pessoal altamente qualificado e especializado. A ***figura 10*** mostra a evolução dos níveis de pessoal na CERT-UE desde o seu início, em 2011, até ao presente.

87 Mais de dois terços dos membros do pessoal da CERT-UE têm contratos a termo certo. O seu salário não é muito competitivo no mercado de especialistas em cibersegurança e, de acordo com a gestão da CERT-UE, tornou-se cada vez mais difícil contratá-los e mantê-los. Quando os salários não são suficientemente atrativos para os candidatos seniores, a CERT-UE deve recorrer à contratação de pessoal júnior e investir tempo na sua formação. Além disso, os contratos têm uma duração máxima de seis anos, o que significa que a CERT-UE não tem outra opção senão dispensar o pessoal contratado quando este se encontra no auge do seu saber-fazer. A rotação da mão de obra foi particularmente elevada em 2020: 21% do pessoal deixou a CERT-UE e não foi possível recrutar substitutos para todos os lugares. No que se refere aos anos anteriores, 9% do pessoal saiu em 2019 e 13% em 2018.

[36] Considerando 7 do Acordo Interinstitucional (AII).

Figura 10 – Recursos e desafios da CERT-UE



Fonte: TCE, com base em dados da CERT-UE.

88 A administração da CERT-UE sublinhou que, atualmente, a sua equipa dedicada à peritagem forense digital e à resposta a incidentes está sobrecarregada e as suas outras equipas não conseguem responder às necessidades. Em consequência, a CERT-UE foi obrigada a reduzir as atividades. Por exemplo, a CERT-UE não efetua atualmente avaliações da maturidade das suas "partes" devido à falta de recursos. O serviço de "alertas de atividade suspeita" da CERT-UE foi introduzido mais tarde do que o previsto, novamente devido à escassez de recursos. Além disso, várias "partes" entrevistadas mencionaram o longo período de tempo que tiveram de esperar para aceder aos serviços da CERT-UE.

89 Até à data, as limitações de recursos obrigaram a CERT-UE a centrar-se, em especial, na proteção de infraestruturas informáticas convencionais, localizadas em instalações físicas, das principais ameaças provenientes de grupos (normalmente apoiados por Estados-nações) que representam ameaças persistentes avançadas. No entanto, de acordo com a sua administração, o alargamento do perímetro informático das EUIBA (que inclui agora a computação em nuvem, os dispositivos móveis e as ferramentas de teletrabalho) necessita de maior acompanhamento e proteção, e as ameaças de menor nível (como a cibercriminalidade e o *ransomware*) também exigem mais atenção.

90 O Acordo Interinstitucional não prevê que a CERT-UE disponha de capacidade operacional vinte e quatro horas por dia, sete dias por semana. A CERT-UE não dispõe atualmente de recursos ou do quadro adequado em termos de recursos humanos que lhe permitam funcionar fora das horas de expediente de forma permanente e estruturada, embora os ataques de cibersegurança não se limitem a este horário. No que diz respeito às próprias EUIBA, apenas 35 das 65 EUIBA inquiridas têm um responsável informático contactável fora do horário de trabalho.

91 Para financiar as operações da CERT-UE, o comité diretor aprovou, em 2012, um modelo de acordo de nível de serviço (ANS). Todas as "partes" recebem serviços de base gratuitos e podem adquirir serviços alargados, mediante a assinatura de um ANS. O orçamento da CERT-UE para 2020 ascendeu a 3 745 000 euros, dos quais 6% foram financiados pelo orçamento da UE e 94% por ANS. No entanto, as "partes" são muito heterogéneas: algumas dispõem de requisitos de segurança informática consolidados, enquanto outras têm orçamentos de TI modestos e um nível muito baixo de maturidade em matéria de cibersegurança. Por este motivo, os debates sobre o ANS resultam numa combinação de requisitos de segurança elevados no caso de algumas EUIBA e numa relativa falta de vontade ou capacidade de contribuir por parte de outras.

92 Além disso, os ANS têm de ser renovados individualmente todos os anos. Além de constituir um encargo administrativo, esta circunstância cria problemas de fluxo de tesouraria, uma vez que a CERT-UE não dispõe de fundos provenientes em simultâneo de todos os ANS. Por outro lado, as agências podem pôr termo aos ANS em qualquer momento. Esta situação pode criar um círculo vicioso em que, devido à perda de receitas, a CERT-UE tem de reduzir os seus serviços e não consegue acompanhar a procura, o que, por sua vez, incita outras EUIBA a porem termo aos seus ANS e a mudarem para prestadores de serviços privados. Tendo em conta estas considerações, o modelo de financiamento atual não é ideal para garantir um nível de serviço estável e adequado.

93 Confrontado com um panorama de ciberameaças em rápida evolução (ver pontos ***06*** e ***80***), o comité diretor da CERT-UE, na sua reunião de 19 de fevereiro de 2020, aprovou uma proposta estratégica para que a CERT-UE alargue os seus serviços de cibersegurança e desenvolva "capacidades operacionais plenas". A proposta foi acompanhada de uma análise das necessidades da CERT-UE em termos de pessoal e financiamento, que concluiu que a CERT-UE precisaria de 14 lugares de administrador permanentes suplementares, adicionados progressivamente ao longo do período de 2021-2023. A CERT-UE funcionaria, então, a plena capacidade a partir de 2023. De acordo com esta proposta, em termos de financiamento, a CERT-UE teria de aumentar o seu orçamento em 7,6 milhões de euros durante o período de 2021-2023, atingindo 11,3 milhões de euros até 2024.

94 No entanto, apesar de aprovarem a proposta estratégica relativa à disponibilização dos recursos adicionais à CERT-UE, as EUIBA ainda não chegaram a acordo sobre as modalidades práticas, em primeiro lugar para o período intercalar de 2021-2023 e, em segundo lugar, a longo prazo, após a entrada em vigor do futuro regulamento relativo à cibersegurança (ver ponto ***12***).

Conclusões e recomendações

95 O Tribunal concluiu que a comunidade das instituições, organismos e agências da UE (EUIBA) não alcançou um nível de preparação cibernética proporcional às ameaças. O trabalho do Tribunal mostra que as EUIBA têm diferentes níveis de maturidade em matéria de cibersegurança e, uma vez que estão frequentemente interligadas entre si e com organizações públicas e privadas dos Estados-Membros, as fragilidades de uma EUIBA neste domínio podem expor várias outras organizações a ciberameaças.

96 O Tribunal constatou que as boas práticas fundamentais em matéria de cibersegurança, incluindo alguns controlos essenciais, nem sempre foram seguidas. Uma boa governação da cibersegurança é essencial para a segurança da informação e dos sistemas informáticos, mas ainda não está em vigor em algumas EUIBA: as estratégias e os planos de segurança informática são, em muitos casos, inexistentes ou não são aprovados pelos quadros superiores, as políticas de segurança nem sempre são formalizadas e as avaliações de riscos não abrangem todo o ambiente informático. As despesas em cibersegurança são desiguais e, em algumas EUIBA, revelam-se claramente inferiores às dos seus pares de dimensão semelhante (ver pontos ***21*** a ***33***, ***37*** e ***38***).

97 Os programas de formação e de sensibilização para a cibersegurança são um elemento fundamental num quadro eficaz em matéria de cibersegurança. No entanto, apenas 29% das EUIBA ministram formação obrigatória em matéria de cibersegurança aos dirigentes responsáveis por sistemas informáticos que contêm informações sensíveis, e a formação oferecida é frequentemente informal. Nos últimos cinco anos, 55% das EUIBA organizaram uma ou mais campanhas de simulação de *phishing* (ou exercícios semelhantes). Estes exercícios são uma ferramenta importante de formação e sensibilização do pessoal, mas as EUIBA não os utilizam de forma sistemática (ver pontos ***34*** a ***36***). Além disso, nem todas as EUIBA submetem regularmente a sua cibersegurança à prestação de uma garantia independente (ver pontos ***39***a ***44***).

98 A CERT-UE é altamente valorizada pelas EUIBA que serve, mas a sua capacidade está sobrecarregada. A sua carga de trabalho, em termos de informação sobre ameaças e tratamento de incidentes, tem vindo a aumentar rapidamente desde 2018. Os ciberincidentes significativos aumentaram mais de dez vezes. Ao mesmo tempo, as EUIBA nem sempre partilham atempadamente informações sobre incidentes significativos, vulnerabilidades e alterações importantes na sua infraestrutura informática. Esta situação prejudica a eficácia da CERT-UE, pois impede-a de alertar outras EUIBA eventualmente afetadas e pode levar a que incidentes significativos

permaneçam por detetar. Além disso, os recursos da CERT-UE são instáveis e, neste momento, não são proporcionais ao atual nível de ameaça ou às necessidades das EUIBA. Em 2020, o comité diretor da CERT-UE aprovou uma proposta estratégica sobre o fornecimento dos recursos adicionais de que esta necessita, mas as "partes" ainda não chegaram a acordo sobre as modalidades práticas para a disponibilização desses recursos. Consequentemente, o pessoal da CERT-UE não consegue responder às necessidades e é obrigado a reduzir as atividades (ver pontos ***74*** a ***93***).

Recomendação 1 – Melhorar a preparação de todas as EUIBA em matéria de cibersegurança através de regras vinculativas comuns e do aumento de recursos da CERT-UE

A Comissão deve incluir os seguintes princípios na sua futura proposta de regulamento sobre medidas em prol de um elevado nível comum de cibersegurança em todas as EUIBA:

a) os quadros superiores devem assumir a responsabilidade pela governação da cibersegurança, aprovando estratégias de cibersegurança e políticas de segurança fundamentais e nomeando um Diretor da Segurança da Informação independente (ou equivalente);

b) as EUIBA devem dispor de um quadro de gestão dos riscos de segurança informática que abranja a totalidade da sua infraestrutura informática e realizar avaliações de riscos regulares;

c) as EUIBA devem oferecer formação para a sensibilização a todo o pessoal de forma sistemática, incluindo aos dirigentes;

d) as EUIBA devem assegurar auditorias e testes regulares às suas ciberdefesas. As auditorias também incluir a adequação dos recursos consagrados à cibersegurança;

e) as EUIBA devem comunicar sem demora à CERT-UE ciberincidentes significativos e alterações e vulnerabilidades pertinentes no que diz respeito à sua infraestrutura informática;

f) as EUIBA devem aumentar e reservar os recursos orçamentais a atribuir à CERT-UE, em consonância com as necessidades assinaladas na proposta estratégica aprovada pelo seu conselho comité diretor;

g) o regulamento deve incluir disposições para a nomeação de uma entidade, representante de todas as EUIBA, que disponha do mandato e dos meios adequados para controlar o cumprimento das regras comuns em matéria de cibersegurança por parte de todas as EUIBA e para emitir orientações, recomendações e apelos à tomada de medidas.

Prazo de transposição visado: primeiro trimestre de 2023

99 As EUIBA estabeleceram mecanismos de cooperação na área da cibersegurança, mas o Tribunal constatou que as potenciais sinergias não são plenamente exploradas. Existe uma estrutura formalizada para o intercâmbio de informações, com intervenientes e comités com funções complementares. No entanto, a participação de EUIBA de menor dimensão em fóruns interinstitucionais é dificultada pela limitação de recursos, e a representação das agências descentralizadas e das empresas comuns no comité diretor da CERT-UE não é a ideal. O Tribunal constatou igualmente que as EUIBA não partilham sistematicamente entre si informações sobre projetos relacionados com a cibersegurança, avaliações de segurança e outros contratos de serviços, o que pode resultar numa duplicação de esforços e num aumento dos custos. O Tribunal observou dificuldades operacionais no intercâmbio de informações sensíveis não classificadas, através de correio eletrónico encriptado ou de videoconferências, devido à falta de interoperabilidade das soluções informáticas, à existência de orientações inconsistentes sobre o seu uso permitido e à ausência de marcações e regras de tratamento comuns das informações (ver pontos ***45*** a ***63***).

Recomendação 2 – Promover mais sinergias entre as EUIBA em áreas selecionadas

A Comissão, no contexto do Comité Interinstitucional para a Transformação Digital, deve promover as seguintes ações junto das EUIBA:

a) adotar soluções para a interoperabilidade de canais de comunicação seguros, desde o correio eletrónico encriptado até à videoconferência, e defender marcações comuns e regras comuns para o tratamento de informações sensíveis não classificadas;

b) partilhar sistematicamente informações sobre projetos relacionados com a cibersegurança com potencial impacto interinstitucional, avaliações de segurança do *software* e contratos em vigor com fornecedores externos;

c) definir especificações para a contratação pública colaborativa e acordos-quadro para serviços de cibersegurança em que todas as EUIBA possam participar para promover economias de escala.

Prazo de transposição visado: quarto trimestre de 2023

100 A Agência da União Europeia para a Cibersegurança (ENISA) e a CERT-UE são as duas principais entidades encarregadas de apoiar as EUIBA em matéria de cibersegurança. No entanto, devido às limitações de recursos e à atribuição de prioridade a outras áreas, não conseguiram prestar às EUIBA todo o apoio de que estas necessitam, em especial no que diz respeito ao desenvolvimento de capacidades das EUIBA que apresentam menos maturidade em matéria de cibersegurança (ver pontos ***64*** a ***93***).

Recomendação 3 – Aumentar o foco da CERT-UE e da ENISA nas EUIBA com menos maturidade

A CERT-UE e a ENISA devem:

a) identificar as áreas prioritárias em que as EUIBA necessitam de maior apoio, por exemplo, através de avaliações da maturidade;

b) executar ações de desenvolvimento de capacidades, em conformidade com o memorando de entendimento.

Prazo de transposição visado: quarto trimestre de 2022

O presente relatório foi adotado pela Câmara III, presidida por Bettina Jakobsen, Membro do Tribunal de Contas, no Luxemburgo, em 22 de fevereiro de 2022.

Pelo Tribunal de Contas

Klaus-Heiner Lehne
Presidente

Anexos

Anexo I – Lista das EUIBA inquiridas

Nome da EUIBA	Tipo
Parlamento Europeu (PE)	Instituição (artigo 13º, nº 1, do Tratado UE)
Conselho da União Europeia e Conselho Europeu (SGC)	Instituição (artigo 13º, nº 1, do Tratado UE)
Comissão Europeia	Instituição (artigo 13º, nº 1, do Tratado UE)
Tribunal de Justiça da União Europeia (TJUE)	Instituição (artigo 13º, nº 1, do Tratado UE)
Banco Central Europeu (BCE)	Instituição (artigo 13º, nº 1, do Tratado UE)
Tribunal de Conta Europeu (TCE)	Instituição (artigo 13º, nº 1, do Tratado UE)
Serviço Europeu para a Ação Externa (SEAE)	Organismo (artigo 27º, nº 3, do Tratado UE)
Comité Económico e Social Europeu (CESE) e Comité das Regiões Europeu (CR)[37]	Organismos (artigo 13º, nº 4, do Tratado UE)
Banco Europeu de Investimento (BEI)	Organismo (artigo 308º do TFUE)
Autoridade Europeia do Trabalho (AET)	Agência descentralizada
Agência da União Europeia de Cooperação dos Reguladores da Energia (ACER)	Agência descentralizada
Gabinete do Organismo de Reguladores Europeus das Comunicações Eletrónicas (Gabinete do Orece)	Agência descentralizada
Instituto Comunitário das Variedades Vegetais (ICVV)	Agência descentralizada
Agência Europeia para a Segurança e a Saúde no Trabalho (EU-OSHA)	Agência descentralizada
Agência Europeia da Guarda de Fronteiras e Costeira (Frontex)	Agência descentralizada
Agência da União Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça (eu-LISA)	Agência descentralizada
Agência da União Europeia para o Asilo	Agência descentralizada
Agência da União Europeia para a Segurança da Aviação (AESA)	Agência descentralizada
Autoridade Bancária Europeia (EBA)	Agência descentralizada

[37] O CESE e o CR são considerados uma EUIBA.

Nome da EUIBA	Tipo
Centro Europeu de Prevenção e Controlo das Doenças (ECDC)	Agência descentralizada
Centro Europeu para o Desenvolvimento da Formação Profissional (Cedefop)	Agência descentralizada
Agência Europeia dos Produtos Químicos (ECHA)	Agência descentralizada
Agência Europeia do Ambiente (AEA)	Agência descentralizada
Agência Europeia de Controlo das Pescas (AECP)	Agência descentralizada
Autoridade Europeia para a Segurança dos Alimentos (EFSA)	Agência descentralizada
Fundação Europeia para a Melhoria das Condições de Vida e de Trabalho (Eurofound)	Agência descentralizada
Agência da União Europeia para o Programa Espacial [em substituição de: Agência do GNSS Europeu – GSA] (EUSPA)	Agência descentralizada
Instituto Europeu para a Igualdade de Género (EIGE)	Agência descentralizada
Autoridade Europeia dos Seguros e Pensões Complementares de Reforma (EIOPA)	Agência descentralizada
Agência Europeia da Segurança Marítima (EMSA)	Agência descentralizada
Agência Europeia de Medicamentos (EMA)	Agência descentralizada
Observatório Europeu da Droga e da Toxicodependência (OEDT)	Agência descentralizada
Agência da União Europeia para a Cibersegurança (ENISA)	Agência descentralizada
Agência da União Europeia para a Formação Policial (CEPOL)	Agência descentralizada
Serviço Europeu de Polícia (Europol)	Agência descentralizada
Agência Ferroviária da União Europeia (AFE)	Agência descentralizada
Autoridade Europeia dos Valores Mobiliários e dos Mercados (ESMA)	Agência descentralizada
Fundação Europeia para a Formação (ETF)	Agência descentralizada
Agência dos Direitos Fundamentais da União Europeia (FRA)	Agência descentralizada
Instituto da Propriedade Intelectual da União Europeia [conhecido como IHMI até 23 de março de 2016] (EUIPO)	Agência descentralizada
Conselho Único de Resolução (CUR)	Agência descentralizada
Agência da União Europeia para a Cooperação Judiciária Penal (Eurojust)	Agência descentralizada
Centro de Tradução dos Organismos da União Europeia (CdT)	Agência descentralizada
Procuradoria Europeia	Agência descentralizada
Instituto Europeu de Inovação e Tecnologia (EIT)	Organismo criado ao abrigo da I&I
Empresa Comum para a Investigação da Gestão do Tráfego Aéreo no Céu Único Europeu (SESAR)	Empresa comum ao abrigo do TFUE
Empresa Comum Componentes e Sistemas Eletrónicos para uma Liderança Europeia (ECSEL)	Empresa comum ao abrigo do TFUE

Nome da EUIBA	Tipo
Empresa Comum Pilhas de Combustível e Hidrogénio 2 (FCH2)	Empresa comum ao abrigo do TFUE
Empresa Comum para a execução da iniciativa tecnológica conjunta sobre medicamentos inovadores 2 (IMI2)	Empresa comum ao abrigo do TFUE
Empresa Comum Clean Sky 2 (Cleansky 2)	Empresa comum ao abrigo do TFUE
Empresa Comum Bioindústrias (BBI)	Empresa comum ao abrigo do TFUE
Empresa Comum Iniciativa Tecnológica Conjunta Shift2Rail (S2R)	Empresa comum ao abrigo do TFUE
Empresa Comum para a Computação Europeia de Alto Desempenho (EuroHPC)	Empresa comum ao abrigo do TFUE
Empresa Comum Europeia para o ITER – Fusão para a Produção de Energia (F4E)	Empresa comum ao abrigo do TFUE
Missão de Aconselhamento da União Europeia sobre a Reforma do Setor da Segurança Civil na Ucrânia (EUAM Ucrânia)	Missão civil (PCSD)
Missão da União Europeia de Assistência à Gestão Integrada das Fronteiras na Líbia (EUBAM Líbia)	Missão civil (PCSD)
Missão PCSD da União Europeia no Níger (EUCAP Sael Níger)	Missão civil (PCSD)
Missão de Observação da União Europeia na Geórgia (EUMM Geórgia)	Missão civil (PCSD)
Gabinete de Coordenação da União Europeia para o Apoio à Polícia Palestiniana (EUPOL COPPS)	Missão civil (PCSD)
Missão de Aconselhamento da UE na República Centro-Africana (EUAM RCA)	Missão civil (PCSD)
Missão de Aconselhamento da UE no Iraque (EUAM Iraque)	Missão civil (PCSD)
Missão de Assistência Fronteiriça da União Europeia para o Posto de Passagem de Rafa (EUBAM Rafa)	Missão civil (PCSD)
Missão PCSD da União Europeia no Mali (EUCAP Sael Mali)	Missão civil (PCSD)
Missão da União Europeia de Reforço das Capacidades na Somália (EUCAP Somália)	Missão civil (PCSD)
Missão da União Europeia para o Estado de Direito no Kosovo (EULEX Kosovo)	Missão civil (PCSD)

Anexo II – Informações adicionais sobre os principais comités interinstitucionais

Comité Interinstitucional para a Transformação Digital (ICDT)

O ICDT é um fórum para o intercâmbio de informações e a promoção da cooperação no domínio das TI. Foi criado em maio de 2020, substituindo o antigo Comité Interinstitutionnel de l'Informatique (CII). É composto pelos dirigentes dos serviços de TI das EUIBA. O ICDT integra um subgrupo de cibersegurança (CSSG do ICDT) que tem por missão promover a cooperação entre as EUIBA em matéria de cibersegurança e servir de fórum para o intercâmbio de informações.

O poder de decisão do ICDT limita-se a questões que não afetam "a forma como as instituições cumprem a sua missão" e não "interferem com a governação de cada instituição". No que diz respeito a decisões que vão além das suas competências, o ICDT pode fazer recomendações ao colégio de Secretários-Gerais das instituições e organismos da UE.

De acordo com o mandato do ICDT, os seus membros são representantes de cada instituição e organismo da UE e existe um representante nomeado pelas agências da UE (ICTAC). O Secretariado-Geral do Conselho preside atualmente ao ICDT.

Subgrupo de cibersegurança do ICDT (CSSG do ICDT)

O CSSG do ICDT, na sua configuração atual, foi criado em setembro de 2020, substituindo o subgrupo permanente de segurança do antigo CII. Em comparação com o seu antecessor, o CSSG do ICDT tem uma abordagem mais estruturada, ambiciosa e orientada para os resultados. As suas atividades são levadas a cabo por grupos de trabalho (GT) que se reúnem regularmente e se centram em questões comuns fundamentais:

- GT1 "Normas comuns, avaliação comparativa e maturidade"
- GT2 "Métodos e ferramentas de plataformas de partilha e contratos"
- GT3 "Segurança em nuvem"
- GT4 "Desenvolvimento de talentos em cibercompetências"
- GT5 "Cibersensibilização"
- GT6 "Segurança das videoconferências"

De acordo com o mandato do CSSG, o seu secretariado-geral é responsável pelo acompanhamento regular da evolução das atividades dos grupos de trabalho e a comunicação de informações a este respeito. Apresenta relatórios periódicos ao presidente e ao vice-presidente do subgrupo de cibersegurança do ICDT, recolhendo regularmente contributos dos coordenadores dos grupos de trabalho. No final de cada ano, o CSSG deve também apresentar um relatório de síntese das atividades.

A Comissão preside atualmente ao CSSG do ICDT, com um representante do ICTAC como Vice-Presidente. Embora o CSSG não tenha poder de decisão, pode recomendar ao ICDT decisões sobre questões pertinentes.

Rede de agências

A Rede de agências da UE (EUAN) é uma rede informal criada pelos chefes das agências da UE em 2012. Atualmente, a EUAN inclui 48 agências descentralizadas da UE e empresas comuns. O seu objetivo é disponibilizar aos membros da rede uma plataforma de intercâmbio e cooperação sobre áreas de interesse comum. O Comité Consultivo para as TIC (ICTAC) é o subgrupo da EUAN encarregado de promover a cooperação no domínio das TIC, incluindo na área da cibersegurança.

Comité Consultivo para as Tecnologias da Informação e da Comunicação (ICTAC)

O ICTAC promove a cooperação entre as agências e as empresas comuns no domínio das TIC. Visa encontrar soluções viáveis e económicas para problemas comuns, trocar informações e adotar posições comuns, sempre que adequado. De acordo com o caderno de encargos do ICTAC, as assembleias gerais que reúnem todos os seus membros são realizadas duas vezes por ano. São também organizadas reuniões mensais regulares entre os representantes do ICTAC nos grupos de trabalho do CSSG, o representante do ICTAC no CSSG e a "troica" do ICTAC. A troica é composta pelos atuais, antigos e futuros presidentes do ICTAC (cada presidente exerce funções durante o período de um ano). A função da troica é apoiar o atual presidente em todos os assuntos relacionados com a sua função, incluindo a sua substituição, se as circunstâncias assim o exigirem.

Siglas e acrónimos

AII: acordo interinstitucional

ANS: acordo de nível de serviço

CERT-UE: Equipa de Resposta a Emergências Informáticas para as instituições e agências da UE

CISO: Diretor da Segurança da Informação

CSIRT: Equipa de Resposta a Incidentes de Segurança Informática

CSSG do ICDT: Subgrupo de Cibersegurança do Comité Interinstitucional para a Transformação Digital

DG DIGIT: Direção-Geral da Informática

DG Recursos Humanos e Segurança: Direção-Geral dos Recursos Humanos e da Segurança

ENISA: Agência da União Europeia para a Cibersegurança

EUAN: Rede de Agências da União Europeia

EUIBA: instituições, organismos e agências da União Europeia

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

ICDT: Comité Interinstitucional para a Transformação Digital

ICTAC: Comité Consultivo de Tecnologias da Informação e Comunicação

ISACA: Information Systems Audit and Control Association

ITCB: Conselho das Tecnologias da Informação e da Cibersegurança

SRI: segurança das redes e da informação

TIC: tecnologias da informação e da comunicação

Glossário

Ameaça persistente avançada: ataque em que um utilizador não autorizado acede a um sistema ou rede para roubar dados sensíveis e aí permanece durante um longo período de tempo.

Ciberespaço: o ambiente em linha global em que as pessoas, o *software* e os serviços comunicam através de redes de computadores e outros dispositivos conectados.

Ciberespionagem: ato ou prática de obtenção de segredos e informações da Internet, redes ou computadores individuais sem a autorização e o conhecimento do detentor das informações.

Cibersegurança: medidas para proteger as redes e infraestruturas informáticas, bem como as informações que contêm, contra ameaças externas.

Engenharia social: no domínio da segurança da informação, manipulação psicológica para incitar as pessoas a fazerem algo ou partilharem informações confidenciais.

Equipa de Resposta a Emergências Informáticas das EUIBA: plataforma de intercâmbio de informações e de coordenação da resposta a incidentes cujos clientes ("as partes") são as instituições, organismos e agências da UE.

Exercício de equipa de segurança ofensiva: simulação realista de ciberataques utilizando o elemento da surpresa e técnicas recentemente observadas no mundo real, centrando-se em objetivos específicos através de múltiplas linhas de ataque.

***Phishing*:** envio de mensagens de correio eletrónico que supostamente têm origem numa fonte de confiança para incitar os destinatários a abrir ligações maliciosas ou a partilhar dados pessoais.

Teste de penetração: método de avaliação da segurança de um sistema informático que consiste em tentar violar as suas garantias de segurança com as ferramentas e técnicas normalmente utilizadas pelos adversários.

Respostas da Comissão

https://www.eca.europa.eu/pt/Pages/DocItem.aspx?did=60922

Respostas da CERT-UE e da ENISA

https://www.eca.europa.eu/pt/Pages/DocItem.aspx?did=60922

Cronologia

https://www.eca.europa.eu/pt/Pages/DocItem.aspx?did=60922

DIREITOS DE AUTOR

PDF	ISBN 978-92-847-7616-0	1977-5822	doi:10.2865/513091	QJ-AB-22-003-PT-N
HTML	ISBN 978-92-847-7574-3	1977-5822	doi:10.2865/373282	QJ-AB-22-003-PT-Q

O número de ciberataques a instituições, organismos e agências da UE (EUIBA) está a aumentar acentuadamente. Uma vez que as EUIBA estão profundamente interligadas, as fragilidades de uma delas podem expor outras a ciberameaças. O Tribunal examinou se as EUIBA dispõem de mecanismos adequados para se protegerem contra as ciberameaças. Constatou que, globalmente, o seu nível de preparação não é proporcional às ameaças e que estas entidades têm níveis muito diferentes de maturidade em matéria de cibersegurança. Recomenda que a Comissão deve promover a melhoria do nível de preparação das EUIBA, propondo a introdução de regras de cibersegurança vinculativas e o aumento dos recursos da Equipa de Resposta a Emergências Informáticas para as instituições e agências da UE (CERT-UE), bem como incentivar mais sinergias entre as EUIBA. A CERT-UE e a Agência da União Europeia para a Cibersegurança devem aumentar o foco nas EUIBA com menos maturidade.

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/Pages/ContactForm.aspx
Sítio Internet: eca.europa.eu
Twitter: @EUAuditors