Contact Committee

Comité de Contacto

das Instituições Superiores de Controlo da União Europeia

Compêndio de auditoria

A cibersegurança na UE e nos seus Estados Membros

auditorias da resiliência dos sistemas de informação e das infraestruturas digitais de importância crítica aos ciberataques

Relatórios de auditoria
publicados entre 2014 e 2020

PT

Dezembro de 2020

O Comité de Contacto das Instituições Superiores de Controlo (ISC) da União Europeia (UE) constitui um fórum de debate e resolução de assuntos relacionados com a auditoria pública na UE. Através do reforço do diálogo e da cooperação entre os seus membros, o Comité de Contacto contribui para aumentar a eficácia da auditoria externa das políticas e programas da UE. Contribui igualmente para promover a prestação de contas, melhorar a gestão financeira da UE e consolidar a sua boa governação, em benefício de todos os cidadãos da União.

Contacto: www.contactcommittee.eu

Índice

Página

Índice

Nota introdutória

Caros leitores,

A digitalização e a utilização crescente das tecnologias da informação em todos os aspetos do nosso quotidiano estão a abrir um mundo novo de oportunidades. Por sua vez, o risco de as pessoas, as empresas e as autoridades públicas serem vítimas da cibercriminalidade ou de um ciberataque aumentou, tal como o impacto que daí advém para a sociedade e a economia.

Na UE, a cibersegurança é uma prerrogativa dos Estados-Membros. A UE tem um papel a desempenhar na instituição de um quadro regulamentar comum no mercado único da União e na criação de condições para que os Estados-Membros trabalhem em conjunto num contexto de confiança mútua.

A cibersegurança e a nossa autonomia digital passaram a ser questões de importância estratégica para a UE e os seus Estados-Membros. Subsistem insuficiências na governação da cibersegurança nos setores público e privado em todos os Estados-Membros, ainda que em diferentes graus, o que prejudica a nossa capacidade de limitar e, sempre que necessário, responder aos ciberataques. A desinformação, muitas vezes orquestrada fora da UE, está a aumentar, como comprovou mais uma vez, no último ano, a pandemia de COVID-19. Este fenómeno constitui uma ameaça, que não podemos ignorar, à coesão nas nossas sociedades e à confiança dos cidadãos nos nossos sistemas democráticos.

Em 2018, um inquérito das Instituições Superiores de Controlo (ISC) na UE revelou que, até então, cerca de metade destas instituições não tinha auditado a cibersegurança. Desde então, as nossas ISC têm intensificado o seu trabalho de auditoria neste domínio, incidindo especialmente na proteção de dados, no grau de preparação dos sistemas para ciberataques e na proteção dos sistemas de serviços públicos essenciais. Como é natural, nem todas as auditorias podem ser tornadas públicas, uma vez que, em alguns casos, podem estar relacionadas com informações sensíveis (de segurança nacional).

Durante o último ano, a crise provocada pela COVID-19 tem posto à prova o tecido económico e social das nossas sociedades. Tendo em conta a nossa dependência das tecnologias da informação, uma "cibercrise" poderá muito bem ser a próxima pandemia. Devemos estar preparados e reforçar a resiliência dos sistemas de informação e das infraestruturas digitais de importância crítica aos ciberataques.

Esperamos que a síntese apresentada neste compêndio estimule ainda mais o interesse dos auditores públicos de toda a União por este domínio tão importante.

Klaus-Heiner Lehne

Presidente do Tribunal de Contas Europeu
Presidente do Comité de Contacto
Chefe do projeto

Síntese

I A cibersegurança e a nossa autonomia digital passaram a ser **questões de importância estratégica para a UE e os seus Estados-Membros** e, à medida que o nível de ameaça aumenta, devemos intensificar os esforços para proteger os sistemas de informação e as infraestruturas digitais de importância crítica contra os ciberataques. A cibersegurança diz respeito não apenas aos serviços públicos, à defesa ou aos sistemas de saúde, mas também à proteção dos dados pessoais, modelos de negócio e propriedade intelectual. Em última análise, a cibersegurança destina-se a proteger as nossas sociedades democráticas, a nossa independência enquanto europeus e a forma como vivemos em conjunto.

II A primeira secção deste terceiro compêndio do Comité de Contacto apresenta **as implicações da cibersegurança**. Descreve os desafios que a cibersegurança coloca às autoridades públicas, às empresas e às pessoas e salienta o novo fenómeno da desinformação, que constitui uma ameaça crescente à coesão social nas nossas sociedades e nos nossos sistemas democráticos. Explica, além disso, as competências e os intervenientes da UE em matéria de cibersegurança, a estratégia e a legislação da União, bem como o financiamento da UE disponível neste domínio.

III A segunda parte do compêndio apresenta uma síntese dos **resultados de auditorias selecionadas realizadas pelas ISC de 12 Estados-Membros participantes e pelo Tribunal de Contas Europeu**, publicadas entre 2014 e 2020. Estas auditorias abordaram aspetos importantes da cibersegurança, como a proteção dos dados privados, a integridade dos centros nacionais de dados, a segurança das instalações de serviços públicos e a aplicação das estratégias nacionais de cibersegurança num sentido mais lato.

IV A terceira parte do compêndio contém **fichas informativas pormenorizadas sobre as auditorias selecionadas**, bem como uma sinopse de outras auditorias publicadas pelas ISC sobre o tema da cibersegurança.

PARTE I – A cibersegurança no contexto europeu

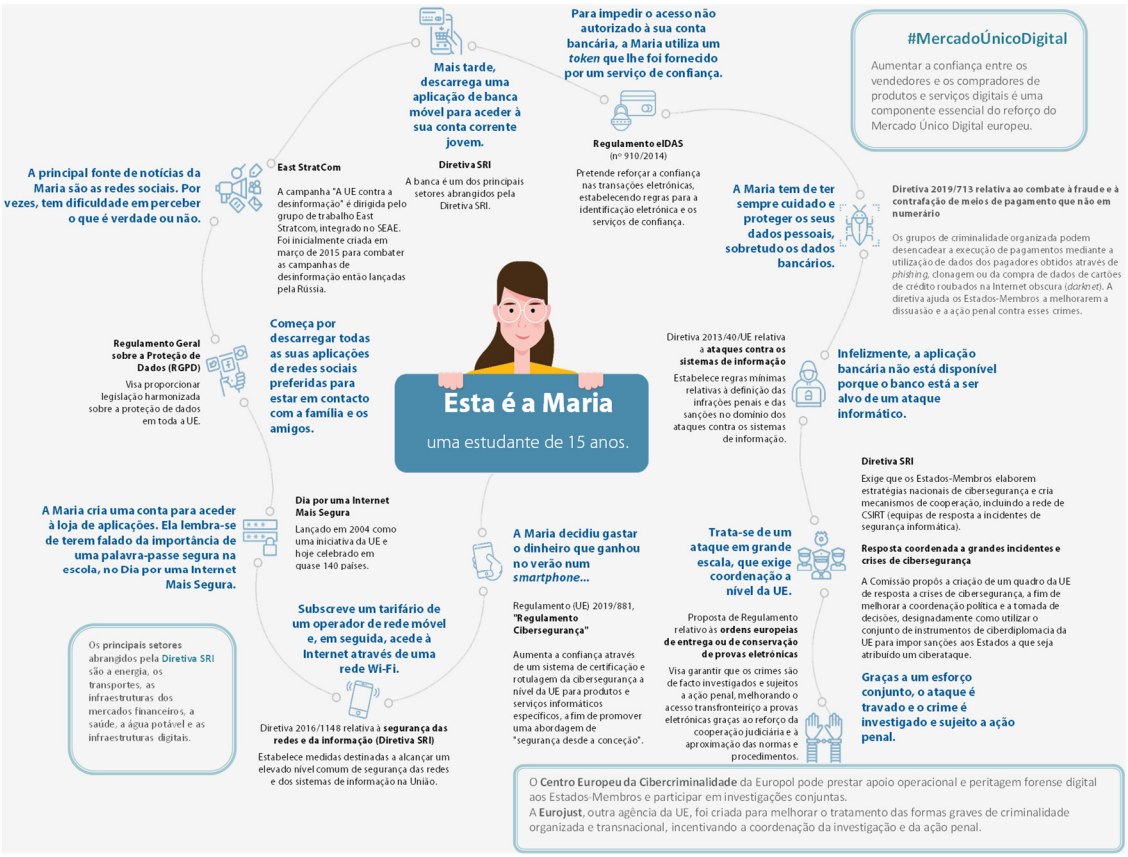
O que é a cibersegurança?

1 Não existe uma **definição** normalizada e universal **de cibersegurança**. No presente documento, cibersegurança refere-se às **atividades necessárias para proteger de ciberameaças as redes e os sistemas de informação, os seus utilizadores e outras pessoas afetadas**. A cibersegurança implica prevenir e detetar ciberincidentes, responder-lhes e recuperar dos mesmos. Estes incidentes podem ser propositados ou não e vão desde a divulgação acidental de informações até aos ataques a empresas e infraestruturas de importância crítica, ao roubo de dados pessoais ou à interferência em processos democráticos e até eleitorais ou a campanhas gerais de desinformação destinadas a influenciar os debates públicos.

A cibersegurança afeta o quotidiano de todos os cidadãos da UE

2 A cibersegurança afeta o quotidiano dos cidadãos da UE quando utilizam dispositivos informáticos pessoais como *smartphones*, redes Wi-Fi, redes sociais ou serviços bancários eletrónicos. Em 2020, mais do que nunca, a questão já não é saber se vão ocorrer ciberataques, mas como e quando vão ocorrer. Esta questão diz respeito a todos: **pessoas, empresas e autoridades públicas**. A ***imagem 1*** ilustra a forma como a UE apoia a cibersegurança e criou um quadro para proteger as atividades eletrónicas diárias dos cidadãos contra os ciberataques. A proteção de sistemas de informação e infraestruturas digitais de importância crítica contra os ciberataques tornou-se um desafio estratégico.

Imagem 1 – Apoio da UE à cibersegurança no quotidiano dos seus cidadãos



Fonte: TCE, ícones elaborados por Pixel perfect de https://flaticon.com.

Existem numerosos tipos de ameaças à cibersegurança

3 Os numerosos tipos de ameaças à cibersegurança que as nossas sociedades enfrentam podem ser classificados em função **daquilo que fazem aos dados – divulgação, alteração, destruição ou negação de acesso –** ou dos princípios basilares de segurança da informação que violam (ver ***figura 1***).

Figura 1 – Tipos de ameaças e princípios de segurança da informação que estas colocam em risco

Cadeado = sem impacto na segurança; ponto de exclamação = risco para a segurança.

Fonte: TCE, com base num estudo do Parlamento Europeu[1].

4 Sempre que um dispositivo se liga à Internet ou a outros dispositivos, aumenta a designada "superfície de ataque" de cibersegurança. O crescimento exponencial da "Internet das coisas" (IdC), a computação em nuvem, os megadados e a digitalização da indústria têm sido acompanhados pelo aumento da exposição das vulnerabilidades, permitindo que os autores dos ataques visem cada vez mais vítimas. A variedade dos tipos de ataques e a sua crescente sofisticação fazem com que seja difícil acompanhar o ritmo[2]. A ***caixa 1*** descreve exemplos de **possíveis ciberataques**.

[1] Parlamento Europeu, *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, estudo realizado para a Comissão LIBE, setembro de 2015.

[2] ENISA, *ENISA Threat Landscape Report 2017*, 18 de janeiro de 2018.

Caixa 1

Tipos de ciberataques

O ***malware*** (*software* malicioso) é concebido para provocar danos em dispositivos ou redes, podendo incluir vírus, cavalos de Troia, *ransomware* (*software* de sequestro), *worms* (vermes), *adware* (*software* de publicidade não solicitada) e *spyware* (*software* espião, como o NotPetya).

O ***ransomware*** encripta os dados, impedindo que os utilizadores acedam aos ficheiros até que seja pago um resgate, geralmente numa criptomoeda, na falta do qual é desencadeada uma ação. Segundo a Europol, os ataques de *ransomware* são prevalentes a todos os níveis e houve uma explosão na variedade deste tipo de ataques nos últimos anos (por exemplo, Wannacry[3]).

Os **ataques distribuídos de negação de serviço** (DDoS), que tornam os serviços ou recursos indisponíveis através do envio em massa de mais pedidos do que esse serviço ou recurso consegue tratar, também estão a aumentar, tendo um terço das organizações enfrentado este tipo de ataques em 2017[4].

Os **ataques na Internet** constituem um método atrativo através do qual os perpetradores podem iludir as vítimas utilizando sistemas e serviços da Internet como vetor da ameaça. Assim, abrangem uma vasta superfície de ataque, por exemplo fornecendo URL ou *scripts* maliciosos a fim de direcionar o utilizador ou a vítima para o sítio Web pretendido ou levá-lo a descarregar conteúdo malicioso (ataques de bebedouro, ataques de descarregamento não intencional) e **injetando** código malicioso num sítio Internet legítimo mas comprometido para roubar informações (ou seja, roubo por formulários) para obter vantagens financeiras ou roubar informações[5].

Os utilizadores podem ser manipulados para, involuntariamente, realizarem uma ação ou divulgarem informações confidenciais. Este ardil pode ser utilizado para o roubo de dados ou a ciberespionagem e é conhecido como **engenharia social**. Existem diferentes formas de o conseguir, sendo um dos métodos mais comuns o ***phishing***, em que mensagens eletrónicas que aparentemente provêm de uma fonte fidedigna enganam os utilizadores e levam-nos a revelar informações ou clicar em ligações que infetam os dispositivos mediante o descarregamento de *malware*. Mais de metade dos Estados-Membros comunicou estar a realizar investigações sobre ataques deste tipo a redes[6].

As ameaças mais nefastas são, possivelmente, as **ameaças persistentes avançadas** (APA), em que agressores sofisticados se envolvem a longo prazo na vigilância e no roubo de dados, por vezes com intuitos destrutivos. A sua finalidade é manterem-se discretos durante o máximo de tempo possível. Estas ameaças estão

muitas vezes associadas a Estados e visam setores particularmente sensíveis como a tecnologia, a defesa e as infraestruturas de importância crítica. Considera-se que este tipo de **ciberespionagem** representa pelo menos um quarto de todos os ciberincidentes[7].

O impacto económico dos ciberataques é significativo

5 A ameaça **dos ciberataques e da cibercriminalidade** tornou-se um grande problema nos últimos anos. Em 2016, 80% das empresas da UE já tinham sido alvo de pelo menos um incidente de cibersegurança[8]. Em 2018, 40% dos participantes num inquérito a organizações que utilizam a robótica ou a automatização afirmaram que a perturbação das operações seria a consequência mais grave de um ciberataque aos seus sistemas. No entanto, apesar de conhecerem os ciber-riscos de perturbação, as empresas não dispõem, muitas vezes, de sistemas para os combater[9].

6 Desde então, continuaram a aumentar o número de ciberataques, a sua gravidade e os seus custos financeiros. A cibercriminalidade, na medida em que é possível estimar o seu **impacto financeiro**, custará à economia mundial **6 biliões de dólares por**

---

[3] O *ransomware WannaCry* tirou proveito das vulnerabilidades de um protocolo do Microsoft Windows que permitia tomar o controlo à distância de qualquer computador. Depois de descobrir esta vulnerabilidade, a Microsoft distribuiu um *patch* (remendo), mas centenas de milhares de computadores não tinham sido atualizados e muitos deles foram posteriormente infetados. *Fonte:* A. Greenberg, *Hold North Korea Accountable for Wannacry — and the NSA, too*, WIRED, 19 de dezembro de 2017.

[4] Europol, *Internet Organised Crime Threat Assessment 2018*.

[5] ENISA, *ENISA Threat Landscape 2020 – Web-based attacks*, 20 de outubro de 2020.

[6] Europol, ver acima, 2018.

[7] *European Centre for International Political Economy*, *Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?*, documento ocasional nº 2/18, fevereiro de 2018.

[8] Europol, *Internet Organised Crime Threat Assessment 2017*.

[9] PWC, *Global State of Information Security* (GSISS), *Survey – Strengthening digital society against cyber shocks*, 2017.

ano até 2021, contra os 3 biliões de dólares estimados em 2015[10], no contexto de um PIB mundial estimado de 138 biliões de dólares em 2020. Os custos da cibercriminalidade incluem danos e destruição de dados, roubo de dinheiro, perda de produtividade, roubo de propriedade intelectual, roubo de dados pessoais e financeiros, perturbação da atividade corrente após os ataques, bem como danos de reputação. Segundo as estimativas do Comité Europeu do Risco Sistémico (CERS), o custo médio dos ciberincidentes aumentou 72% entre 2015 e 2020[11].

7 A cibercriminalidade **afeta de forma diferente os diversos setores económicos**, como demonstra um estudo recente, de 2020[12]: foi o fenómeno de fraude mais perturbador nos governos e nas administrações públicas, no setor da tecnologia, da comunicação social e das telecomunicações e no setor da saúde (ver ***caixa 2***); foi igualmente o segundo fenómeno de fraude mais perturbador no setor financeiro e no setor industrial e transformador.

[10] *Cybersecurity Ventures*, *2019 Official Annual Cybercrime Report*, patrocinado pelo Herjavec Group, 2019.

[11] CERS, Comité Europeu do Risco Sistémico, *Systemic cyber risk*, fevereiro de 2020.

[12] PWC, *Fighting fraud: A never-ending battle PwC's Global Economic Crime and Fraud Survey*, 2020.

Caixa 2

Doentes finlandeses em psicoterapia alvo de chantagem com dados médicos pessoais roubados entre 2018 e 2019

Doentes de uma grande clínica de psicoterapia na Finlândia, com sucursais em todo o país, foram contactados individualmente por um chantagista em 2020, na sequência do roubo dos dados pessoais dos doentes em novembro de 2018 e de uma outra possível violação em março de 2019. Aparentemente, os dados incluíam registos de identificação pessoal e notas sobre as questões abordadas nas sessões de psicoterapia.

O chantagista exigiu à clínica e aos doentes que lhe pagassem resgates em *bitcoin* para não divulgar os dados publicamente. Este incidente levou o Governo finlandês a realizar uma reunião de emergência[13].

8 Em 2019, a Europol[14] salientou novamente a **persistência e a tenacidade de algumas das principais ameaças de cibersegurança**:

- os ataques de *ransomware* continuam a ser a principal ameaça; são cada vez mais precisos, mais lucrativos e mais lesivos em termos económicos. Enquanto o *ransomware* proporcionar um rendimento relativamente fácil aos cibercriminosos e continuar a provocar danos e perdas financeiras significativos, deverá continuar a ser a principal ameaça de cibercriminalidade;
- o *phishing* e os protocolos de ambiente de trabalho remoto vulneráveis são os principais vetores primários de infeção por *malware*;
- os dados continuam a ter muita importância para a cibercriminalidade, enquanto alvo preferencial, mercadoria e fator facilitador.

[13] BBC News, *Therapy patients blackmailed for cash after clinic data breach*, 26 de outubro de 2020.

[14] EUROPOL, *INTERNET organised crime threat assessment (IOCTA)*, 2019.

9 De igual modo, no seu **relatório de 2020 sobre os principais incidentes na UE e no mundo**[15], a Agência da União Europeia para a Cibersegurança (ENISA) apresenta vários exemplos de incidentes de cibersegurança (ver ***caixa 3***).

Caixa 3

Agência da União Europeia para a Cibersegurança (ENISA): incidentes de cibersegurança em 2019-2020

A plataforma de correio eletrónico verifications.io foi alvo de uma grande violação de dados devido a uma base de dados MongoDB não protegida. Foram expostos dados de mais de 800 milhões de mensagens de correio eletrónico que continham informações sensíveis, incluindo elementos de identificação.

Mais de 770 milhões de endereços de correio eletrónico e 21 milhões de palavras-passe exclusivas foram expostos num conhecido fórum de pirataria informática alojado pelo serviço de computação em nuvem MEGA1. Este caso tornou-se a recolha mais significativa de credenciais pessoais violadas de sempre, designada por "*Collection #1*".

O Citrix, um prestador de serviços de computação em nuvem e de virtualização, foi vítima de um ciberataque direcionado. Para conseguirem aceder aos sistemas do Citrix, os autores dos ataques exploraram várias vulnerabilidades cruciais do *software*, como a CVE-2019-19781, utilizando uma técnica designada por "*password spraying*".

O iNSYNQ19, um prestador de serviços de alojamento em nuvem, sofreu um ataque de *ransomware* que impediu os clientes de acederem aos seus dados durante mais de uma semana, obrigando-os a utilizar cópias de segurança locais.

10 Segundo a Europol, os ciberataques concebidos para provocar **danos duradouros** duplicaram nos primeiros seis meses de 2019, principalmente no setor transformador. Ao contrário dos ataques de *ransomware* convencionais, estes ataques são atos de sabotagem que apagam ou danificam de forma irreversível dados de empresas (ver ***caixa 4***).

[15] ENISA, *Main incidents in the EU and worldwide – January 2019 to April 2020*, outubro de 2020.

Caixa 4

Ransomware destrutivo: os ataques "GermanWiper" de 2019

Em 2019, foi detetado um conjunto de ataques de *ransomware* contra empresas ativas na Alemanha. Designado por *GermanWiper*, este *ransomware* consegue substituir os ficheiros infetados por zeros e uns, impossibilitando assim a recuperação dos ficheiros. O *ransomware* propaga-se através de campanhas de *phishing* por correio eletrónico e visou, em especial, pessoal dos recursos humanos de empresas de topo, sendo incorporado em candidaturas a emprego falsas[16].

A sensibilização para as ameaças à cibersegurança está a crescer à medida que estas se tornam mais frequentes

11 Não obstante, até recentemente, a consciência e o reconhecimento destes riscos eram ainda bastante reduzidos. Em 2017, 69% das empresas da UE não tinham perceção da sua **exposição a ciberameaças**[17], ou tinham apenas uma perceção básica, e 60% nunca tinham feito uma estimativa das **potenciais perdas financeiras**[18]. Além disso, de acordo com um inquérito global realizado em 2018, um terço das organizações preferiria pagar um resgate ao *hacker* do que investir na segurança da informação[19].

---

16 *Cybersecurity Insiders*, *GermanWiper Ransomware attack warning for Germany*, sem data.

17 Comissão Europeia, *Factsheet on cybersecurity*, setembro de 2017.

18 Estas perdas podem incluir: perda de receitas; custos de reparação de sistemas danificados; responsabilidades potenciais por informações ou recursos roubados; incentivos à retenção de clientes; subida dos prémios de seguro; aumento dos custos de proteção (novos sistemas, funcionários, formação); potencial regularização de custos de conformidade ou litigância.

19 NTT Security, *Risk: Value 2018 Report*.

12 O **Eurobarómetro de 2020 sobre os comportamentos dos europeus face à cibersegurança**[20] identifica a crescente sensibilização, e preocupação, dos cidadãos da UE:

- os inquiridos que utilizam a Internet estão tendencialmente mais preocupados com a utilização abusiva dos seus dados pessoais (46%), a segurança dos seus pagamentos em linha (41%), a impossibilidade de inspecionar artigos ou solicitar aconselhamento a uma pessoa real ou o risco de não receberem os bens ou serviços que adquirem em linha (22% em ambos os casos);
- mais de três quartos (76%) dos inquiridos creem que o risco de serem vítimas da cibercriminalidade está a aumentar. Contudo, bastante menos (52%) consideram que conseguem proteger-se suficientemente, o que representa uma descida de nove pontos percentuais em relação a 2018;
- ainda assim, pouco mais de metade dos inquiridos (52%) consideram estar bem informados sobre a cibercriminalidade, mas apenas 11% afirmam sentir-se muito bem informados.

A cibersegurança é importante para a coesão social e a estabilidade política

Uma nova ameaça: a cibersegurança e a desinformação

13 A propagação de **desinformação** deliberada, sistemática e em larga escala **constitui um sério desafio estratégico para as nossas democracias**[21]. A desinformação e as "notícias falsas" são suscetíveis de dividir as sociedades, disseminar a desconfiança e até pôr em causa a coesão social e a confiança nos processos democráticos (ver ***caixa 5***).

[20] Comissão Europeia, *Special Eurobarometer 499 – Europeans' attitudes towards cyber security*, janeiro de 2020.

[21] De acordo com o estudo intitulado *The Global Disinformation Order*, da Universidade de Oxford (setembro de 2019), o número de países com campanhas de desinformação política mais do que duplicou, para 70, nos últimos dois anos.

Caixa 5

Desinformação

A Comissão Europeia define a desinformação como informação comprovadamente falsa ou enganadora que é criada, apresentada e divulgada para obter vantagens económicas ou para enganar deliberadamente o público, e que é suscetível de causar um prejuízo público[22]. O prejuízo público pode incluir a fragilização dos processos democráticos ou ameaças a bens públicos, como a saúde, o ambiente e a segurança.

Ao contrário dos conteúdos ilegais (que incluem o discurso de ódio, os conteúdos terroristas e a pornografia infantil), a desinformação abrange conteúdos legais. Por conseguinte, está relacionada com os valores fundamentais da UE de liberdade de expressão e liberdade dos meios de comunicação social. Nos termos da definição da Comissão, a desinformação não abrange publicidade enganosa, erros na comunicação de informações, sátiras, paródias ou notícias e comentários claramente identificados como partidários.

14 As novas tecnologias e *software* permitem propagar a desinformação facilmente e de forma comparativamente barata através **das redes sociais e de outros meios em linha**. A desinformação concentra-se geralmente em temas sensíveis que, por poderem polarizar opiniões e agitar emoções, serão provavelmente mais partilhados. Estes temas incluem as questões de saúde (por exemplo, campanhas contra a vacinação), a migração, as alterações climáticas ou as questões de justiça social.

Campanhas de desinformação de países terceiros para influenciar processos democráticos

15 A desinformação visa polarizar o debate democrático, criar ou intensificar tensões na sociedade e comprometer os sistemas eleitorais e tem um impacto alargado nas sociedades e na segurança da Europa, enfraquecendo, em última instância, a liberdade de opinião e de expressão. A desinformação é frequentemente **patrocinada por intervenientes de países terceiros**, com vista a desestabilizar as nossas sociedades e os nossos sistemas democráticos. Neste contexto, as campanhas de desinformação em larga escala podem também incluir a pirataria informática

[22] Comissão Europeia, *Comunicação – Combater a desinformação em linha*, COM(2018) 236.

contra redes, como sucedeu, por exemplo, na campanha de influência russa no referendo do Reino Unido relativo à saída da União Europeia (ver ***caixa 6***).

Caixa 6

Campanhas de desinformação russas que visam processos de decisão democráticos[23]

Em meados de 2016, intervenientes russos lançaram uma campanha destinada a influenciar o referendo do Reino Unido, de junho de 2016, relativo à saída da UE. Uma análise de *tweets* concluiu que, nas 48 horas anteriores à votação, mais de 150 000 contas russas publicaram *tweets* sobre *#Brexit* e mais de 45 000 mensagens sobre a votação. No dia do referendo, contas russas publicaram 1 102 *tweets* com o marcador *#ReasonsToLeaveEU* (motivos para sair da UE).

16 O combate à desinformação representa um grande desafio, devido à necessidade de alcançar um justo equilíbrio entre a segurança e os nossos direitos e liberdades fundamentais, incentivando a inovação e um mercado aberto. A UE tomou várias medidas para **combater a desinformação**.

- Em 2015, foi criado no SEAE o grupo de trabalho de comunicação estratégica para o Leste **"East StratCom"**, com a finalidade de combater as campanhas de desinformação provenientes da Rússia[24]. Os especialistas louvaram o seu trabalho na promoção das políticas da UE, no apoio aos meios de comunicação social independentes nos países da Vizinhança Europeia e na previsão, rastreamento e combate da desinformação[25].

---

[23] *Park advisors*, *Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age*, Christina Nemr e William Gangware, 2019.

[24] Conclusões do Conselho Europeu, documento EUCO 11/15, de 20 de março de 2015. Desde esta data, foram criados outros dois grupos de trabalho, um para os Balcãs Ocidentais e outro para a Vizinhança do Sul.

[25] Um relatório do *Atlantic Council* defendia que a UE deveria exigir que todos os Estados-Membros nomeassem peritos para o grupo de trabalho. Ver: D. Fried e A. Polyakova, *Democratic Offense Against Disinformation*, 5 de março de 2018.

- Em 2018, a ENISA publicou uma **comunicação relativa ao combate à desinformação em linha**[26]. Algumas das medidas são o aumento da fiabilidade dos conteúdos e o apoio aos esforços para aumentar a literacia quanto a notícias e à comunicação social.

- O Centro Comum de Investigação da Comissão elaborou um **código de conduta autorregulador** e voluntário, baseado nos instrumentos de política em vigor, que foi adotado pelas plataformas em linha e pelo setor da publicidade[27].

- Foi também estabelecida uma **rede** europeia independente **de verificadores de factos**.

Desinformação em período de COVID-19 e resposta da UE

17 A desinformação tem sido também um problema no contexto da **crise sanitária provocada pela COVID-19**[28] (ver exemplos deste tipo de desinformação na ***caixa 7***).

[26] ENISA, *Strengthening Network & Information Security & Protecting Against Online Disinformation ("Fake News")*, abril de 2018

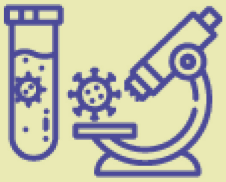
[27] JRC, *The digital transformation of news media and the rise of disinformation and fake news*, relatórios técnicos do JRC, documento de trabalho do JRC sobre a economia digital 2018-02, abril de 2018.

[28] Reuters Institute e Universidade de Oxford, *Types, Sources, and Claims of Covid-19 Misinformation*, abril de 2020.

Caixa 7

Exemplos de desinformação relacionada com a COVID-19 denunciada pela Comissão[29]

Falsas alegações, como "beber lixívia ou álcool puro pode curar a infeção pelo coronavírus": pelo contrário, beber lixívia ou álcool puro pode ser muito perigoso para a saúde. **O centro antivenenos da Bélgica registou um aumento de 15% do número de incidentes relacionados com a lixívia.**



Teorias da conspiração, como a alegação de que o coronavírus é "uma infeção causada pelas elites mundiais para reduzir o crescimento demográfico". As provas científicas são claras: o vírus provém de uma família de vírus originários de animais, entre os quais se contam vírus como o SARS e o MERS.

Alegações sem base científica de que as "instalações 5G estariam a propagar o vírus". Estas teorias, sem qualquer fundamento, estiveram na origem de ataques a postes com antenas 5G.

18 Em março de 2020, a Comissão, a ENISA, a CERT-UE e a Europol emitiram uma **declaração conjunta sobre ameaças relacionadas com a COVID-19**[30], na qual afirmam que intervenientes mal-intencionados estavam a aproveitar-se deliberadamente das circunstâncias difíceis da crise de saúde pública para visar teletrabalhadores, empresas e indivíduos. Além disso, a ENISA desenvolveu campanhas de informação específicas para setores afetados pela desinformação durante a pandemia de COVID-19[31].

[29] Comissão Europeia, *Combater a desinformação relacionada com o coronavírus*, sem data.

[30] *Joint Statement European Commission, ENISA, CERT-EU and Europol, Coronavirus outbreak*, 20 de março de 2020.

[31] ENISA, *Fichas informativas relacionadas com a COVID-19*, 2020.

A verificação de factos é essencial para combater a desinformação

19 A UE também intensificou os esforços no sentido de apoiar os verificadores de factos e os investigadores europeus no domínio da desinformação. Criou, em especial, um **Observatório Europeu dos Meios de Comunicação Digitais**, para examinar e compreender melhor os fenómenos da desinformação: intervenientes importantes, vetores, ferramentas, métodos, dinâmicas de divulgação, objetivos prioritários e o impacto na sociedade. Os projetos financiados pela UE para combater a desinformação incluem também, por exemplo, PROVENANCE, SocialTruth, EUNOMIA e WeVerify.

20 Em 2018, através do seu **Código de Conduta sobre Desinformação**[32], a UE propôs o primeiro conjunto de normas autorregulador a nível mundial para combater a desinformação. Este código voluntário foi assinado por plataformas, pelas principais redes sociais, por anunciantes e pelo setor da publicidade em outubro de 2018. Os signatários são o Facebook, Twitter, Mozilla, Google e associações e membros do setor da publicidade. A Microsoft assinou o Código de Conduta em maio de 2019, e o TikTok fez o mesmo em junho de 2020.

Proteção das eleições de 2019 para o Parlamento Europeu

21 A legitimidade dos nossos sistemas democráticos europeus baseia-se num eleitorado informado que expressa a sua vontade democrática através de **eleições livres e justas**. Por conseguinte, qualquer tentativa de comprometer e manipular a opinião pública de forma maliciosa e intencional representa uma séria ameaça às nossas sociedades. A interferência nas eleições e nas infraestruturas eleitorais pode ter por objetivo influenciar as preferências dos eleitores, a afluência às urnas ou o processo eleitoral em si, incluindo a própria votação, bem como o apuramento e a comunicação dos votos. No seguimento do referendo do Reino Unido, as eleições europeias de 2019 motivaram as primeiras ações coordenadas entre Estados-Membros para **proteger a integridade das eleições democráticas**, quer para o Parlamento Europeu, quer para os parlamentos nacionais.

[32] *EU Code of Practice on Disinformation*, setembro de 2018.

22 Conforme referido anteriormente, a Comissão publicou a **Comunicação – Combater a desinformação em linha: uma estratégia europeia**[33] em abril de 2018. Seguiu-se um **pacote eleitoral**, em setembro de 2018[34], destinado a proteger as eleições da UE e dos Estados-Membros contra a desinformação e os ciberataques. Este pacote centrou-se na proteção de dados, na transparência da publicidade e do financiamento políticos, na cibersegurança e nos atos eleitorais, bem como em sanções contra a violação das regras de proteção de dados pelos partidos políticos. Além disso, realizou-se um **exercício conjunto** para testar o grau de eficácia das práticas de reposta e dos planos de crise dos Estados-Membros e da UE na proteção das eleições para o Parlamento Europeu (ver ***caixa 8***).

[33] Comissão Europeia, *Combater a desinformação em linha: uma estratégia europeia*, COM(2018) 236 final.

[34] Comissão Europeia, *Estado da União 2018*, setembro de 2018.

Caixa 8

ELEx19 – proteção das eleições de 2019 para o Parlamento Europeu[35]

O exercício ELEx19 relativo à resiliência das eleições para o Parlamento Europeu visava identificar formas de prevenir, detetar e atenuar incidentes de cibersegurança que poderiam afetar as eleições de 2019.

Tendo por base vários cenários que incluíam ameaças e incidentes assentes em meios informáticos, este exercício permitiu aos participantes:

obter uma visão geral do nível de resiliência (em termos de políticas adotadas, capacidades disponíveis e competências) dos sistemas eleitorais em toda a UE;

reforçar a cooperação entre as autoridades competentes a nível nacional (incluindo autoridades eleitorais e outros organismos e agências competentes);

testar os planos existentes de gestão de crises, bem como os procedimentos pertinentes para prevenir, detetar, gerir e dar resposta aos ataques à cibersegurança e ameaças híbridas, incluindo campanhas de desinformação;

melhorar a cooperação transfronteiriça e reforçar a ligação com os grupos de cooperação pertinentes a nível da UE (por exemplo, a rede de cooperação para as eleições, o grupo de cooperação SRI, a rede de equipas CSIRT);

detetar todas as outras potenciais lacunas, bem como as medidas adequadas de atenuação dos riscos que deveriam ser aplicadas antes das eleições para o Parlamento Europeu.

Participaram neste exercício mais de 80 representantes dos Estados-Membros da UE, juntamente com observadores do Parlamento Europeu, da Comissão e da Agência da UE para a Cibersegurança.

[35] ENISA, *EU Member States test their cybersecurity preparedness for fair and free 2019 EU elections*, 5 de abril de 2019.

23 Por fim, em dezembro de 2018, o Conselho Europeu adotou um **Plano de Ação contra a Desinformação**[36] para assegurar uma resposta coordenada e complementar os esforços nacionais. Este plano de ação incluía ações específicas baseadas em quatro pilares: melhorar as capacidades das instituições da União para detetar, analisar e denunciar a desinformação; reforçar a coordenação e as respostas comuns à desinformação; mobilizar o setor privado para o combate à desinformação; sensibilizar as pessoas e reforçar a resiliência da sociedade.

A cibersegurança na UE: competências, intervenientes, estratégias e legislação

A cibersegurança é essencialmente uma responsabilidade dos Estados-Membros

24 Na UE, a cibersegurança é essencialmente uma **responsabilidade dos Estados-Membros**, em especial no âmbito da proteção de informações sensíveis relacionadas com a segurança nacional. Todos os Estados-Membros dispõem de uma **Estratégia Nacional de Cibersegurança**, que os ajuda a combater os riscos passíveis de comprometer a realização dos benefícios económicos e sociais do ciberespaço. No entanto, ainda existem disparidades entre os níveis de capacidade e compromisso dos Estados-Membros em matéria de cibersegurança.

25 A UE tem um papel a desempenhar na instituição de um **quadro regulamentar comum** no mercado único da União e na criação de condições para que os Estados-Membros trabalhem eficazmente em conjunto em diferentes domínios de intervenção em que a cibersegurança é pertinente, como a justiça e os assuntos internos, o mercado único, os transportes, a saúde pública, a política dos consumidores e a investigação. Na política externa, a cibersegurança está patente na diplomacia e é uma parte cada vez maior da política emergente de segurança e defesa da UE.

---

[36] Comissão Europeia, Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, *Plano de Ação contra a Desinformação*, JOIN(2018) 36 final. O plano incide na melhoria das capacidades das instituições da UE para detetar, analisar e denunciar a desinformação; no reforço da coordenação e de respostas comuns; na mobilização do setor privado; na sensibilização e no reforço da resiliência da sociedade.

26 A *caixa 9* descreve os principais **intervenientes a nível da UE** no domínio da cibersegurança.

Caixa 9

Principais intervenientes a nível da UE no domínio da cibersegurança

A **Comissão Europeia** pretende melhorar as capacidades e a cooperação em matéria de cibersegurança, tornar a UE num interveniente mais forte neste domínio e integrar a cibersegurança noutras políticas da UE.

A Comissão é apoiada por várias agências da UE, designadamente a **ENISA**, o **EC3** e a **CERT-UE**. A **Agência da União Europeia para a Cibersegurança** (conhecida como **ENISA** devido à sua designação inicial, Agência Europeia para a Segurança das Redes e da Informação) é essencialmente um organismo consultivo e apoia o desenvolvimento das políticas, o reforço de capacidades e a sensibilização. O **Centro Europeu da Cibercriminalidade (EC3)** da Europol foi criado para reforçar a resposta das autoridades policiais da UE à cibercriminalidade. A Comissão acolhe ainda uma **Equipa de Resposta a Emergências Informáticas (CERT-UE)**, que dá apoio a todas as instituições, órgãos e organismos da União.

O **Serviço Europeu para a Ação Externa (SEAE)** conduz a ciberdefesa, a ciberdiplomacia e a comunicação estratégica, albergando centros de recolha e análise de informações. A **Agência Europeia de Defesa (AED)** tem por finalidade desenvolver as capacidades de ciberdefesa.

A nível da UE, os Estados-Membros intervêm através do **Conselho**, que tem numerosos organismos de coordenação e partilha de informações (entre os quais o Grupo Horizontal das Questões do Ciberespaço). O **Parlamento Europeu** intervém enquanto colegislador.

As **organizações do setor privado**, incluindo as empresas, os organismos de governação da Internet e o meio académico, são parceiros que contribuem para o desenvolvimento e execução das políticas, por exemplo através de uma parceria público-privada contratual (**PPPc**).

A estratégia da UE para o ciberespaço: a cibersegurança constitui uma grande preocupação desde 2013

27 A cibersegurança constitui uma grande preocupação política pelo menos desde 2013, ano em que a Comissão adotou a sua **estratégia para a cibersegurança**[37]. Esta estratégia tem cinco prioridades:

- aumentar a resiliência do ciberespaço;
- reduzir a cibercriminalidade;
- desenvolver a política e as capacidades no domínio da ciberdefesa;
- desenvolver os recursos industriais e tecnológicos para a cibersegurança;
- estabelecer uma política internacional em matéria de ciberespaço em harmonia com os valores fundamentais da UE.

Nos anos seguintes, a questão da cibersegurança também foi incluída noutras estratégias da UE (ver ***caixa 10***).

[37] Comissão Europeia, *Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido*, JOIN(2013) 1 final, 7 de fevereiro de 2013.

Caixa 10

Outras estratégias da UE que abordam a questão da cibersegurança

- a **Agenda Europeia para a Segurança** (2015)[38], que visava melhorar a aplicação da lei e a resposta judicial à cibercriminalidade, principalmente através da renovação ou atualização das políticas e da legislação em vigor;
- a **Estratégia para o Mercado Único Digital** (2015)[39], que visava melhorar o acesso a bens e serviços digitais: para este efeito, é essencial reforçar a segurança, a confiança e a inclusão em linha;
- a **estratégia global da UE** (2016)[40], que estabeleceu um conjunto de iniciativas para reforçar o papel da UE no mundo. A cibersegurança, a par da contestação da desinformação através da comunicação estratégica, constituía um pilar fundamental neste contexto.

28 Além disso, em 2017, a Comissão Europeia e a Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança emitiram uma **comunicação conjunta** ao Parlamento Europeu e ao Conselho **sobre a cibersegurança na UE**[41], na qual solicitaram estruturas mais robustas e eficazes para promover a cibersegurança e responder aos ciberataques nos Estados-Membros, mas também nas próprias instituições, agências e organismos da UE.

29 Em julho de 2020, a Comissão Europeia atualizou a sua agenda de 2015 e adotou a **Estratégia da UE para a União da Segurança**[42] para 2020-2025, identificando a

---

38 Comissão Europeia, *Agenda Europeia para a Segurança*, COM(2015) 185 final, de 28 de abril de 2015.

39 Comissão Europeia, *Estratégia para o Mercado Único Digital na Europa*, COM(2015) 192 final, de 6 de maio de 2015.

40 SEAE, *Visão partilhada, ação comum: uma Europa mais forte. Estratégia global para a política externa e de segurança da União Europeia*, junho de 2016.

41 Comissão Europeia e Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, *Comunicação conjunta – Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE*, JOIN(2017) 450, de 13 de setembro de 2017.

42 Comissão Europeia, *Comunicação sobre a Estratégia da UE para a União da Segurança*, COM(2020) 605 final, de 24 de julho de 2020.

cibersegurança como uma questão de importância estratégica. Nesta estratégia, a Comissão salienta, em especial, as chamadas ameaças híbridas, que implicam ciberataques combinados com campanhas de desinformação, nas quais intervenientes estatais e não estatais de países terceiros atuam de forma concertada com o intuito de manipular o ambiente de informação e atacar as infraestruturas de base.

A legislação da UE em matéria de cibersegurança: a Diretiva Segurança das Redes e da Informação, o RGPD, o Regulamento Cibersegurança e um novo mecanismo de sanções

30 Como principal pilar da estratégia para a cibersegurança de 2013, a **Diretiva Segurança das Redes e da Informação (SRI)**[43], de 2016, é o elemento jurídico central e o primeiro ato legislativo à escala da UE em matéria de cibersegurança. A diretiva visa alcançar um nível mínimo de harmonização de capacidades, obrigando os Estados-Membros a adotarem estratégias nacionais de segurança das redes e dos sistemas de informação e a criarem pontos de contacto únicos e equipas de resposta a incidentes de segurança informática (CSIRT)[44]. Além disso, estabelece requisitos de segurança e de notificação para os operadores de serviços essenciais em setores de importância crítica e para os prestadores de serviços digitais.

31 Os Estados-Membros tinham de transpor **a Diretiva SRI para o direito nacional** até maio de 2018, bem como de identificar os chamados "operadores de serviços essenciais" até novembro de 2018. Cabe à Comissão Europeia avaliar periodicamente a aplicação da diretiva. Entre julho e outubro de 2020, no âmbito do seu objetivo político fundamental de "uma Europa preparada para a era digital", e em consonância com os objetivos da União da Segurança, a Comissão realizou uma consulta, cujos

[43] Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

[44] Estas equipas estão integradas em estruturas de cooperação criadas pela diretiva, a Rede de CSIRT (uma rede composta pelas CSIRT designadas pelos Estados-Membros da UE e pela CERT-UE, cujo secretariado é assegurado pela ENISA) e o Grupo de Cooperação (que apoia e facilita a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros e cujo secretariado é assegurado pela Comissão).

resultados deverão ser utilizados numa primeira avaliação e numa avaliação de impacto *ex post* da Diretiva SRI.

32 Paralelamente, em 2016 entrou em vigor o **Regulamento geral sobre a proteção de dados**[45] (RGPD), que é aplicável desde maio de 2018. O seu objetivo é proteger os dados pessoais dos cidadãos europeus, estipulando regras sobre o seu tratamento e divulgação. São conferidos determinados direitos aos titulares de dados e criadas obrigações por parte dos responsáveis pelo tratamento dos dados (prestadores de serviços digitais) sobre a utilização e transferência de informações.

33 Além disso, o **Regulamento Cibersegurança**[46] introduz o primeiro enquadramento para a certificação da cibersegurança a nível da UE para produtos, serviços e processos das TIC. Desta forma, as empresas que operam na UE terão a vantagem de ter de certificar os seus produtos, serviços e processos de TIC apenas uma vez, sendo os certificados reconhecidos em toda a UE. O Regulamento Cibersegurança da UE também criou a **Agência da União Europeia para a Cibersegurança** (ENISA, que sucede à anterior Agência Europeia para a Segurança das Redes e da Informação), incumbindo-a de aumentar a cooperação operacional a nível da UE ajudando os Estados-Membros, caso estes o solicitem, a tratar os incidentes de cibersegurança e apoiando a coordenação da UE em casos de ciberataques e crises transnacionais em grande escala.

34 Por último, em maio de 2019, o Conselho criou um instrumento jurídico que permite à UE impor **medidas** restritivas específicas **para dissuadir e dar resposta aos ciberataques** que constituam uma ameaça externa à União ou aos seus

[45] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

[46] Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação.

Estados-Membros[47]. Desta forma, a UE tem competência jurídica para aplicar sanções a pessoas ou entidades que:

- sejam responsáveis por ciberataques ou tentativas de ciberataques;
- prestem assistência financeira, técnica ou material ou estejam de qualquer outro modo envolvidas nestes ataques.

Em julho de 2020, o Conselho utilizou primeira vez estas novas prerrogativas (ver ***caixa 11***).

Caixa 11

Uma ação mais robusta: a UE impõe as primeiras sanções de sempre contra ciberataques[48]

Em julho de 2020, o Conselho impôs medidas restritivas contra seis pessoas e três entidades responsáveis por vários ciberataques ou que neles participaram. Trata-se, nomeadamente, da tentativa de ciberataque contra a Organização para a Proibição de Armas Químicas e dos ciberataques publicamente conhecidos como "WannaCry", "NotPetya" e "Operation Cloud Hopper".

As sanções impostas incluem a proibição de viajar e o congelamento de bens. Além disso, é proibido a pessoas e entidades da UE colocarem fundos à disposição das pessoas e entidades incluídas na respetiva lista de sanções.

[47] Decisão (PESC) 2019/797 do Conselho, de 17 de maio de 2019, relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros.

[48] Decisão (PESC) 2020/1127 do Conselho, de 30 de julho de 2020, que altera a referida Decisão (PESC) 2019/797 relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros.

Cibersegurança e ciberdefesa

35 Nos últimos anos, o ciberespaço tornou-se cada vez mais militarizado[49] e belicista[50]. É atualmente considerado o quinto domínio da guerra além de terra, mar, ar e espaço. Em 2014, foi adotado um **Quadro Estratégico da UE para a Ciberdefesa**, que foi atualizado em 2018[51]. Na versão atualizada de 2018, são definidas prioridades que incluem o desenvolvimento das capacidades de ciberdefesa e a proteção das redes de comunicação e informação da Política Comum de Segurança e Defesa (PCSD) da UE. A ciberdefesa faz igualmente parte do quadro de Cooperação Estruturada Permanente e da cooperação UE-NATO.

36 Os casos de utilização do ciberespaço como instrumento político e meio de agressivamente pôr à prova e penetrar a cibersegurança da UE e dos Estados-Membros tornaram-se comuns. Estas atividades de ciberespionagem e pirataria informática – visando administrações centrais, entidades políticas e as instituições da UE para extrair e compilar informações classificadas – sugerem que estão em curso operações sofisticadas de ciberespionagem e manipulação de dados contra a UE e os seus Estados-Membros. O **quadro comum da UE em matéria de luta contra as ameaças híbridas** (2016) visa combater as ciberameaças dirigidas às infraestruturas de importância crítica e aos utilizadores privados, salientando que os ciberataques também podem ser realizados por meio de campanhas de desinformação nas redes sociais[52]. Nesse documento, regista-se também a necessidade de aumentar

---

[49] Centro de Estudos de Política Europeia (CEPE), *Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force*, novembro de 2018.

[50] O *malware* por trás do ataque de *ransomware* WannaCry, cuja autoria foi atribuída à Coreia do Norte pelos Estados Unidos, o Reino Unido e a Austrália, foi inicialmente desenvolvido e guardado pela Agência de Segurança Nacional (NSA) dos Estados Unidos para explorar as vulnerabilidades do Windows.
Fonte: A. Greenberg, WIRED, 19 de dezembro de 2017. Na sequência dos ataques, a Microsoft condenou a prática de os governos guardarem em reserva as vulnerabilidades detetadas em *software* e reiterou o seu apelo à necessidade de uma Convenção de Genebra Digital.

[51] *Quadro Estratégico da UE para a Ciberdefesa (atualização de 2018)*, documento nº 14413/18, 19 de novembro de 2018.

[52] Comissão Europeia/Serviço Europeu para a Ação Externa, *Quadro comum em matéria de luta contra as ameaças híbridas: uma resposta da União Europeia*, JOIN(2016) 18 final, de 6 de abril de 2016.

o conhecimento sobre a situação e de reforçar a cooperação entre a UE e a NATO, que foi consubstanciada nas Declarações Conjuntas UE-NATO de 2016 e 2018[53].

As despesas relacionadas com a cibersegurança na UE são dispersas e tardias

Menos despesas no domínio da cibersegurança na UE-27 do que nos EUA

37 É difícil estimar as despesas públicas no domínio da cibersegurança, devido à sua natureza transversal e ao facto de muitas vezes não ser possível distinguir as despesas com a cibersegurança das despesas gerais com a informática[54]. Não obstante, os dados disponíveis indicam que as **despesas públicas no domínio da cibersegurança** na UE são baixas em termos comparativos:

- em 2020, o orçamento do governo federal dos EUA dedicado apenas à cibersegurança ascendeu a aproximadamente **17,4 mil milhões de dólares**[55];
- comparativamente, as estimativas da Comissão indicam que as despesas públicas no domínio da cibersegurança se situam entre **mil e dois mil milhões de euros** por ano para todos os Estados-Membros da UE (os quais, em conjunto, têm um PIB quase igual ao dos EUA)[56];

[53] Declarações Conjuntas dos Presidentes do Conselho Europeu e da Comissão Europeia e do Secretário-Geral da Organização do Tratado do Atlântico Norte, 8 de julho de 2016 e 10 de julho de 2018.

[54] Comissão Europeia, COM(2018) 630 final, de 12 de setembro de 2018.

[55] Casa Branca, *Cybersecurity budget fiscal year 2020*.

[56] Comissão Europeia, *Commission Staff Working Document: Impact Assessment accompanying the document "Proposal for a Regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027"*, SWD(2018) 305 final, de 6 de junho de 2018.

- estima-se que as despesas públicas de muitos Estados-Membros no domínio da cibersegurança sejam, em percentagem do PIB, **um décimo das dos EUA** ou mesmo inferiores[57].

2014-2020: o financiamento da UE para a cibersegurança dispersou-se por vários instrumentos diferentes

38 De acordo com a Comissão[58], existem pelo menos **dez instrumentos diferentes** ao abrigo do orçamento geral da UE que podem ser utilizados para financiar medidas relacionadas com a cibersegurança (ver na ***caixa 12*** os principais programas em termos financeiros). No total, o financiamento da UE para cibersegurança não militar representou **menos de 200 milhões de euros por ano** durante o período de 2014-2020. Além disso, não existe um instrumento de financiamento a nível da UE que apoie os Estados-Membros na coordenação das suas atividades de cibersegurança.

[57] *The Hague Centre for Strategic Studies*, *Dutch investments in ICT and cybersecurity: putting it in perspective*, dezembro de 2016.

[58] Comissão Europeia, *Impact assessment accompanying the proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres*, SWD(2018) 403 final, 12 de setembro de 2018.

Caixa 12

Programas da UE que apoiam projetos de cibersegurança (2014-2020)

- Os **programas de investigação do Horizonte 2020** da UE atribuíram cerca de 600 milhões de euros a projetos relativos à cibersegurança e à cibercriminalidade no período de 2014-2020, incluindo 450 milhões de euros para a PPPc para a cibersegurança para 2017-2020, com o objetivo de atrair mais 1,8 mil milhões de euros do setor privado;

- os **Fundos Europeus Estruturais e de Investimento (FEEI) preveem** uma contribuição máxima de 400 milhões de euros para investimentos dos Estados-Membros em cibersegurança até ao final de 2020;

- o **Mecanismo Interligar a Europa (MIE)** financiou investimentos num montante aproximado de 30 milhões de euros por ano, incluindo o cofinanciamento das Equipas de Resposta a Emergências Informáticas (CERT) nacionais que os Estados-Membros têm de criar ao abrigo da Diretiva SRI, num montante de aproximadamente 13 milhões de euros por ano, entre 2016 e 2018[59];

- o **Fundo para a Segurança Interna – Polícia** apoia estudos, reuniões de especialistas e atividades de comunicação, num montante que ascendeu a perto de 62 milhões de euros entre 2014 e 2017. No quadro da gestão partilhada, os Estados-Membros podem também beneficiar de subvenções para equipamento, formação, investigação e recolha de dados, às quais recorreram 19 Estados-Membros, num montante total de 42 milhões de euros;

- o **Programa Justiça** disponibilizou 9 milhões de euros para apoio à cooperação judiciária e a tratados de auxílio judiciário mútuo, com ênfase no intercâmbio eletrónico de dados e de informações financeiras.

39 Além disso, foram atribuídos 500 milhões de euros do orçamento da UE ao **Programa Europeu de Desenvolvimento Industrial no domínio da Defesa** em 2019

[59] Artigo 9º, nº 2, da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União ("Diretiva SRI").

e 2020[60]. Este programa visa melhorar a coordenação e a eficiência das despesas dos Estados-Membros neste domínio mediante incentivos ao desenvolvimento conjunto. O seu objetivo é gerar um total de 13 mil milhões de euros de investimento em capacidades de defesa após 2020 através do Fundo Europeu de Defesa, do qual uma parte abrangerá a ciberdefesa. Por último, no âmbito da **Iniciativa para a Segurança Europeia**, o Banco Europeu de Investimento irá disponibilizar, entre 2018 e 2020, 6 mil milhões de euros de financiamento para soluções de dupla utilização (investigação e desenvolvimento/cibersegurança e segurança civil)[61].

2021-2027: o novo Programa Europa Digital

40 No âmbito das suas conclusões de julho de 2020 sobre o novo quadro financeiro plurianual (QFP) para o período de 2021-2027, o Conselho decidiu que o **Programa Europa Digital**[62] investiria nas capacidades digitais estratégicas fundamentais, tais como a computação de alto desempenho, a inteligência artificial e a cibersegurança na UE, complementando outros instrumentos, designadamente o Horizonte Europa e o Mecanismo Interligar a Europa, no apoio à transformação digital da Europa.

41 O Conselho decidiu também afetar 6,8 mil milhões de euros ao Programa Europa Digital no período de 2021-2027, ou seja, aproximadamente **970 milhões de euros por ano**. Trata-se de um aumento considerável em comparação com o período de 2014-2020, mas ainda inferior ao inicialmente proposto pela Comissão (8,2 mil milhões de euros para o mesmo período, com 2 mil milhões de euros dedicados ao reforço do setor da cibersegurança da UE e à proteção global da sociedade, por exemplo, apoiando a aplicação da Diretiva SRI).

---

[60] Comissão Europeia, Regulamento (UE) 2018/1092 do Parlamento Europeu e do Conselho, de 18 de julho de 2018, que estabelece o Programa Europeu de Desenvolvimento Industrial no domínio da Defesa destinado a apoiar a competitividade e a capacidade inovadora da indústria de defesa da União (JO L 200 de 7.8.2018, p. 30).

[61] Banco Europeu de Investimento, *The EIB Group Operating Framework and Operational Plan 2018*, 12.12.2017.

[62] Comissão Europeia, *Europe investing in digital: the Digital Europe Programme*, setembro de 2020.

PARTE II – Síntese dos trabalhos das ISC

Introdução

42 A cibersegurança e a nossa autonomia digital passaram a ser questões de importância estratégica para a UE e os seus Estados-Membros. Subsistem insuficiências na governação da cibersegurança nos setores público e privado em todos os Estados-Membros, ainda que em diferentes graus, o que prejudica a nossa capacidade de limitar e, sempre que necessário, responder aos ciberataques.

43 Contudo, em 2018, um inquérito das Instituições Superiores de Controlo (ISC) na UE revelou que cerca de metade destas instituições nunca tinha auditado o domínio da cibersegurança. Desde então, as ISC têm intensificado o seu trabalho de auditoria neste domínio, incidindo especialmente na proteção de dados, no grau de preparação dos sistemas para ciberataques e na proteção dos sistemas de serviços públicos essenciais, mas examinando também outros temas especialmente relevantes. Como é natural, nem todas as auditorias podem ser tornadas públicas, uma vez que, em alguns casos, podem estar relacionadas com informações sensíveis (de segurança nacional).

44 Atendendo à importância da cibersegurança para o funcionamento das nossas sociedades e instituições políticas, o Comité de Contacto decidiu dedicar o compêndio de auditoria deste ano a este tema. Esta segunda parte apresenta uma síntese dos resultados das auditorias selecionadas realizadas pelas ISC de 12 Estados-Membros participantes e pelo Tribunal de Contas Europeu relativas à cibersegurança. Cada ISC participante contribuiu com um relatório de auditoria selecionado, que é resumido na terceira parte. Este assunto foi objeto de muitas outras auditorias, como demonstram os relatórios adicionais referidos pelas ISC participantes.

Metodologia da auditoria e temas abordados

45 No que se refere ao tipo de auditoria que deu origem aos relatórios sintetizados no presente compêndio, a maior parte das ISC participantes realizou auditorias de resultados sobre assuntos relacionados com a cibersegurança, mas duas (da Polónia e da Hungria) realizaram auditorias de conformidade e uma (o TCE) efetuou uma análise das políticas.

46 Na determinação do método a aplicar, a maior parte das ISC concebeu as suas auditorias de modo a incluir pelo menos duas formas de avaliar o tema da auditoria, que consistiam num exame de documentos estratégicos ou políticas definidas de alto

nível (por exemplo, nacionais), num exame dos procedimentos utilizados para avaliar a sua conformidade com a metodologia COBIT instituída (ver ***caixa 13***) ou ainda numa análise da eficácia dos sistemas de gestão informática em vigor. Uma ISC (o Tribunal de Contas neerlandês) utilizou até *hackers* bem-intencionados para testar a eficácia dos sistemas de cibersegurança no controlo das fronteiras e nas estruturas de importância crítica de gestão da água. A ***caixa 14*** resume esquematicamente os métodos e as técnicas que as diferentes ISC utilizaram no seu trabalho de auditoria.

Caixa 13

O que é a metodologia COBIT?

A metodologia COBIT (*Control Objectives for Information and Related Technology*) é um quadro de boas práticas e procedimentos reconhecidos para gestão e governação informática definido pela ISACA (*Information Systems Audit and Control Association*), que ajuda cada organização a alcançar objetivos estratégicos mediante uma utilização eficaz dos recursos disponíveis e a minimização dos riscos informáticos. A metodologia COBIT interliga a governação das empresas com a governação informática, designadamente associando os objetivos da empresa aos objetivos informáticos, definindo métricas e modelos de maturidade para medir a realização dos objetivos e definindo as responsabilidades dos proprietários das empresas e dos processos informáticos.

47 Os temas abordados durante as auditorias da cibersegurança variaram consideravelmente. Algumas ISC auditaram domínios de interesse público muito específicos: a ISC dos Países Baixos, por exemplo, auditou a cibersegurança das suas proteções marítimas e sistemas de gestão da água, que são vitais para o país. Outras, como as ISC irlandesa e húngara, abordaram questões mais horizontais, como a execução da estratégia nacional de cibersegurança e a proteção de dados pessoais e dos recursos de dados nacionais. No entanto, todas as ISC se debruçaram sobre questões que podem ter um impacto negativo nos serviços ou infraestruturas públicos.

48 As ISC estónia e lituana reconheceram a importância estratégica dos recursos de dados nacionais enquanto elementos cruciais da segurança nacional e da proteção da integridade nacional contra ciberataques externos. A ISC dinamarquesa dedicou especificamente uma auditoria à avaliação da segurança de quatro organismos públicos contra ataques de *ransomware*. As ISC neerlandesa, polaca e portuguesa auditaram a eficácia de diferentes sistemas informáticos que apoiam os controlos nas fronteiras (respetivamente no aeroporto de Schiphol; no Alto-Comando dos Guardas

de Fronteira e no Ministério dos Assuntos Internos e da Administração na Polónia; nas fronteiras portuguesas), abordando assim também a segurança no interior da UE.

Período de auditoria

49 Os relatórios de auditoria selecionados para o presente compêndio foram publicados entre 2014 e 2020. Na sua maioria, têm um período de auditoria de dois ou mais anos, embora quatro auditorias (Dinamarca, Estónia, França e Portugal) tenham incidido sobre períodos de um ano.

Objetivos das auditorias

50 As diferentes ISC que participaram neste compêndio concentraram-se em riscos diversos durante o seu trabalho de auditoria. Os riscos abordados nos respetivos contributos foram os seguintes: ameaças aos direitos individuais dos cidadãos da UE mediante uma utilização indevida dos seus dados pessoais, o risco de as instituições não conseguirem prestar um serviço público importante ou terem um desempenho limitado e consequências graves para a segurança pública, o bem-estar e a economia nos Estados-Membros, bem como para a cibersegurança na UE. Pelo menos quatro ISC (estónia, húngara, neerlandesa e portuguesa) abordaram três ou mais destes temas nos seus relatórios de auditoria incluídos no presente compêndio.

51 A cibersegurança continua a ser uma competência dos Estados-Membros. No entanto, uma vez que a legislação da UE se tornou mais abrangente e mais específica ao longo do tempo, a maior parte das instituições e dos organismos auditados pelas ISC já contribuem para concretizar os objetivos estratégicos de cibersegurança da UE, ainda que em diferentes medidas. Por exemplo, o *Office of the Comptroller and Auditor General* da Irlanda auditou a aplicação da Diretiva Segurança das Redes e da Informação da UE, que visa melhorar a resiliência de redes e sistemas de informação essenciais, e prestou aconselhamento nesse sentido. De igual forma, a auditoria da ISC húngara abordou a vertente da conformidade com as diretivas da UE em vigor.

52 A ***caixa 14*** indica também os casos em que os efeitos da auditoria contribuíram para aumentar a ciber-resiliência das entidades auditadas ou reduzir a cibercriminalidade, ou em que poderiam contribuir para o cumprimento dos principais objetivos da estratégia da UE para a cibersegurança, designadamente desenvolver as políticas de ciberdefesa e reforçar as competências, melhorar o desenvolvimento de

tecnologias e alcançar progressos na cooperação a nível internacional. Na maioria dos casos, as recomendações apresentadas pelas ISC abordaram mais do que dois objetivos estratégicos da UE.

53 Além disso, o trabalho de auditoria das ISC identificou lacunas de segurança ou de aplicação que levaram as instituições auditadas a envidar esforços adicionais. Por exemplo, ainda durante o trabalho de auditoria, quatro instituições auditadas na Dinamarca começaram a aplicar vários controlos de segurança virados para o futuro, a fim de aumentar significativamente o nível de proteção contra ataques de *ransomware*, a desenvolver capacidades de defesa e a aumentar a ciber-resiliência, reduzindo assim a sua exposição à cibercriminalidade no futuro.

54 É possível constatar também que foram formuladas recomendações a vários níveis de gestão e responsabilidade, dirigidas a administrações centrais, a ministérios e organismos a nível operacional ou a proprietários de sistemas informáticos.

Caixa 14

Síntese dos trabalhos de auditoria das ISC para os contributos incluídos no compêndio (primeira parte)

Principal domínio de incidência		Dinamarca	Estónia	Irlanda	França	Letónia	Lituânia	Hungria	Países Baixos	Polónia	Portugal	Finlândia	Suécia	UE (TCE)
Tipo de auditoria	Resultados	✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	
	Conformidade							✓		✓				
	Análise													✓
Método de auditoria	Análise de políticas	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓
	Análise de procedimentos	✓	✓		✓		✓	✓		✓	✓	✓		
	Análise de sistemas	✓			✓	✓	✓	✓	✓	✓	✓		✓	
	Avaliação da robustez mediante testes diretos								✓		✓			
Ameaças avaliadas	Impacto nos direitos individuais		✓		✓			✓			✓			✓
	Impacto em infraestruturas ou serviços públicos	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Impacto na segurança nacional		✓	✓		✓	✓	✓	✓		✓			
	Impacto na segurança na UE	✓							✓		✓			✓

Síntese dos trabalhos de auditoria das ISC para os contributos incluídos no compêndio (segunda parte)

Principal domínio de incidência		Dinamarca	Estónia	Irlanda	França	Letónia	Lituânia	Hungria	Países Baixos	Polónia	Portugal	Finlândia	Suécia	UE (TCE)
Objetivos estratégicos de cibersegurança da UE abrangidos	Aumento da ciber-resiliência	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
	Redução da cibercriminalidade	✓					✓							✓
	Desenvolvimento das políticas e capacidades no domínio da defesa	✓	✓	✓		✓	✓	✓	✓	✓				✓
	Desenvolvimento dos recursos tecnológicos				✓	✓			✓				✓	
	Aumento da cooperação internacional (políticas)			✓				✓						✓
Nível do destinatário das recomendações	Administração central	✓	✓				✓					✓	✓	✓
	Operacional (ministérios e organismos)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Proprietários de sistemas informáticos	✓			✓			✓	✓	✓				

Principais observações de auditoria

55 As secções seguintes sintetizam as principais observações de auditoria apresentadas pelas ISC.

Auditorias de resultados

56 A **ISC da Dinamarca, *Rigsrevisionen*,** verificou se determinadas instituições públicas essenciais dispunham de uma proteção satisfatória contra o *ransomware*. As instituições públicas são alvos frequentes de ciberataques, e o *ransomware* é atualmente uma das maiores ameaças à cibersegurança. A auditoria incidiu sobre a Autoridade dos Dados de Saúde, o Ministério dos Negócios Estrangeiros, a *Banedanmark* (rede ferroviária) e a Agência de Gestão de Emergências da Dinamarca. Estas quatro instituições foram selecionadas por serem responsáveis pela prestação de serviços essenciais na saúde, nos negócios estrangeiros, nos transportes e na preparação para emergências, domínios em que a garantia de acesso aos dados pode ter uma importância crítica. A auditoria concluiu que as quatro instituições não dispunham de uma proteção satisfatória contra o *ransomware*. Os trabalhos de auditoria demonstraram que as quatro instituições não tinham aplicado vários controlos de segurança comuns destinados a atenuar os ataques. A auditoria concluiu que era importante estas instituições ponderarem a aplicação de controlos de segurança virados para o futuro, a fim de aumentar a sua resiliência a ataques de *ransomware*.

57 A **ISC da Estónia, *Riigikontroll*,** reconheceu que a preservação da independência nacional exige não apenas a defesa física do território, mas também a proteção dos ativos digitais de importância primordial para o Estado. Os ativos digitais que mais necessitam de proteção são os dados relativos aos cidadãos, ao território e à legislação. No entanto, é necessário proteger também os dados referentes à propriedade, aos bens imóveis e aos direitos das pessoas residentes na Estónia. A ISC da Estónia analisou a possibilidade de ciberameaças em caso de agravamento dos problemas de segurança. Estes cenários de risco, conjugados com um aumento do número de incidentes relacionados com a segurança da informação, nomeadamente ciberataques e fugas de dados, poderão comprometer os dados e as bases de dados mais importantes para o Estado. Por conseguinte, a auditoria analisou a forma como o Estado determinava quais os dados e as bases de dados que considerava cruciais para

garantir a segurança nacional. A auditoria concluiu que, apesar da aplicação do ISKE[63], um sistema de segurança de base em três níveis que é obrigatório nos organismos públicos, existiam deficiências significativas na garantia da segurança da informação em várias bases de dados cruciais.

58 A **ISC da Irlanda, *Office of the Comptroller and Auditor General*,** analisou os progressos realizados nas medidas de cibersegurança após a criação, em 2011, do Centro Nacional de Cibersegurança, gerido pelo Ministério das Comunicações, da Ação Climática e do Ambiente. Este centro tem como principais objetivos proteger as redes públicas, ajudar as empresas e as pessoas a protegerem os seus próprios sistemas e salvaguardar infraestruturas nacionais de importância crítica. A auditoria concluiu que, embora o Centro Nacional de Cibersegurança desempenhasse uma função crucial, o nível dos recursos que lhe foram atribuídos nos primeiros quatro anos de funcionamento foi significativamente inferior ao inicialmente previsto e que a orientação estratégica global do centro não incluía um plano estratégico. Além disso, era necessária maior clareza quanto aos papéis específicos dos organismos envolvidos na investigação dos cibercrimes e dos incidentes de segurança nacional. Por outro lado, ainda não tinham sido aplicados os requisitos da Diretiva Segurança das Redes e da Informação da UE relativos à elaboração de uma estratégia nacional.

59 A **ISC de França, *Cour des comptes*,** analisou a *Parcoursup*, uma nova plataforma digital que constitui uma fonte de informação sobre os cursos universitários disponíveis e os requisitos de acesso, tendo como objetivo aumentar a correspondência entre as aptidões e os resultados académicos dos estudantes do ensino secundário e os conteúdos dos cursos de ensino superior. A auditoria concluiu que o Governo conseguiu centralizar o acesso a todos os estudos pós-secundários através da plataforma digital para fazer face à expansão do ensino superior. Contudo, a nova *Parcoursup* consistia numa reformulação apressada do sistema anterior, sem alterações estruturais substantivas. Por conseguinte, não foram corrigidas as vulnerabilidades do sistema de informação em termos de segurança, desempenho e robustez. A plataforma continua sujeita a riscos significativos no que diz respeito à qualidade e continuidade do serviço público e à segurança dos dados pessoais.

[63] O ISKE é uma norma de segurança da informação desenvolvida para o setor público da Estónia; esta norma é obrigatória para as organizações da administração nacional e local que trabalham com bases de dados ou registos.

60 A **ISC da Letónia, *Valsts Kontrole*,** concluiu uma auditoria de resultados relativa à eficiência das infraestruturas públicas das tecnologias da informação e comunicação (TIC). A auditoria tinha como objetivo verificar se a administração pública possuía uma abordagem unificada para uma gestão eficiente das infraestruturas das TIC e se as instituições tinham avaliado os benefícios da centralização. A auditoria concluiu que, devido à relutância das autoridades em gerir centralmente as infraestruturas das TIC, tinham sido criadas várias salas de servidores, que aumentaram significativamente os custos de manutenção. Existiam ameaças de segurança na maior parte das salas de servidores, já que os centros de dados não estavam suficientemente protegidos contra o acesso físico e os riscos ambientais. Além disso, não tinha sido introduzida nas instituições qualquer prática de avaliação regular da opção mais económica entre assegurar internamente a manutenção das infraestruturas das TIC, cooperar com outra instituição ou subcontratar a manutenção das TIC. A auditoria recomendou um sistema de acompanhamento regular que permitisse avaliar toda a administração pública com um sistema único.

61 A **ISC da Lituânia, *Valstybės kontrolė*,** reconheceu a importância dos recursos eletrónicos de informação de importância crítica do Estado, nomeadamente na gestão das finanças públicas, na administração fiscal e nos cuidados de saúde. A perda de informações de importância crítica e a indisponibilidade dos sistemas de informação correspondentes pode ter consequências graves para a segurança pública, o bem-estar e a economia. A auditoria tinha como objetivo avaliar a gestão (controlo geral) e a maturidade dos recursos de informação de importância crítica do Estado. Identificou problemas sistémicos na elaboração e na execução da política relativa aos recursos de informação do Estado, bem como no mecanismo de gestão desses recursos. A auditoria concluiu que o baixo nível de maturidade dos recursos de informação de importância crítica do Estado refletia insuficiências na elaboração e na execução da política relativa aos recursos de informação do Estado, que tornavam esses recursos mais vulneráveis. Para aumentar a segurança dos recursos de informação do Estado, era necessário melhorar o mecanismo de gestão.

62 Em 2018, o **Tribunal de Contas dos Países Baixos** decidiu realizar auditorias da cibersegurança em setores de importância crítica para a sociedade. Os dois primeiros setores auditados foram a gestão da água e os controlos automatizados nas fronteiras: o primeiro é essencial para um país que se encontra maioritariamente abaixo do nível do mar e o segundo é importante devido à posição do aeroporto de Amesterdão-Schiphol como aeroporto central internacional e porta de entrada no país. O Ministério das Infraestruturas e da Gestão da Água classificou várias estruturas

hídricas geridas pela Direção-Geral das Obras Públicas e Gestão da Água (a entidade auditada) como "partes cruciais" do setor da gestão da água. Muitos dos sistemas informáticos utilizados no funcionamento das estruturas de importância crítica de gestão da água remontam às décadas de 1980 e 1990, um período em que, normalmente, a cibersegurança não era tida em conta. O Ministério da Defesa e o Ministério da Justiça e da Segurança são conjuntamente responsáveis pelos controlos nas fronteiras realizados pelos guardas de fronteira neerlandeses no aeroporto de Schiphol. Os guardas de fronteira utilizam sistemas informáticos dos dois ministérios. Estes sistemas são essenciais para as operações nos aeroportos e são utilizados para tratar dados altamente sensíveis, constituindo, por isso, um alvo apetecível para ciberataques que visam a sabotagem, a espionagem ou a manipulação dos controlos nas fronteiras. A auditoria examinou se as entidades auditadas estavam preparadas para responder a ciberameaças e se o faziam com eficácia. No caso das estruturas de gestão da água, a entidade auditada teria ainda de melhorar a sua deteção e resposta para cumprir as suas próprias metas de cibersegurança. No que diz respeito aos controlos nas fronteiras, a auditoria concluiu que as medidas de cibersegurança não eram adequadas nem estavam preparadas para o futuro.

63 O **Tribunal de Contas de Portugal** auditou os sistemas de informação que suportam a concessão, emissão e utilização do passaporte eletrónico português (PEP), designadamente no controlo automatizado de passageiros através da leitura de dados biométricos nas fronteiras portuguesas. A auditoria verificou o cumprimento do direito da UE e nacional, das normas internacionais e das orientações para a concessão, emissão e utilização do PEP, incluindo a adequação do quadro jurídico nacional. Examinou a eficácia dos principais processos associados ao ciclo de vida do PEP, em especial os associados à concessão, emissão e utilização do PEP. A auditoria examinou também os aspetos críticos do desempenho dos sistemas de informação, em especial a satisfação de requisitos de segurança relativos ao Sistema de Informação do Passaporte Eletrónico Português (SIPEP).

64 A **ISC da Finlândia, *Valtiontalouden tarkastusvirasto*,** verificou se a ciberproteção na administração central era tão eficaz e eficiente em termos de custos quanto possível. A auditoria incidiu sobre a forma de gestão da cibersegurança da administração central. As entidades auditadas incluíram as autoridades que regulam a ciberproteção na administração central (o Gabinete do Primeiro-Ministro, o Ministério das Finanças e o Ministério dos Transportes e das Comunicações) e as autoridades responsáveis por tarefas centralizadas de ciberproteção e serviços informáticos centralizados na administração central. No Governo finlandês, a responsabilidade pela

ciberproteção é descentralizada, sendo cada órgão institucional responsável pela sua própria cibersegurança. A auditoria recomendou que o Ministério das Finanças definisse e aplicasse um modelo abrangente de gestão operacional para os casos de incidentes de cibersegurança nos serviços das TIC da administração central. O Ministério das Finanças deveria também procurar formas de ter em conta a cibersegurança no financiamento dos serviços ao longo do seu ciclo de vida e melhorar o conhecimento situacional operacional, incumbindo as autoridades de denunciar ciberviolações ao Centro de Cibersegurança.

65 A **ISC da Suécia, *Riksrevisionen*,** abordou a incidência de sistemas informáticos obsolescentes na administração central, a fim de avaliar se o Governo e as autoridades tinham tomado medidas adequadas para evitar que os sistemas informáticos se tornem um obstáculo a uma digitalização eficaz. A auditoria identificou sistemas informáticos obsolescentes num número elevado de organismos públicos. Em muitos dos organismos auditados, um ou mais sistemas informáticos fundamentais para a atividade encontravam-se obsolescentes e uma parte significativa dos organismos examinados não abordava corretamente o desenvolvimento e a administração do apoio informático. Uma parte significativa dos organismos não possuía uma descrição global da ligação entre estratégias, processos operacionais e sistemas. Concluiu-se globalmente que a maior parte dos organismos ainda não conseguia responder eficazmente aos problemas associados a sistemas informáticos obsolescentes. A ISC sueca considera que este problema é de tal forma grave e generalizado que constitui um obstáculo à prossecução de uma digitalização eficiente da administração pública.

Auditorias de conformidade realizadas no domínio da cibersegurança

66 A **Instituição Superior de Controlo da Hungria** reconheceu que a segurança dos recursos de dados nacionais constitui um interesse fundamental da sociedade tendo em vista a preservação e a proteção dos valores nacionais. Garantir um reforço da segurança dos dados pessoais e públicos nos recursos de dados nacionais da Hungria é essencial para reforçar a confiança dos cidadãos no Estado e assegurar um funcionamento contínuo e harmonioso da administração pública. A finalidade da auditoria de conformidade relativa à proteção de dados consistia em avaliar se o quadro regulamentar e operacional da proteção de dados tinha sido instituído na Hungria e se as grandes organizações de gestão de dados tinham cumprido os requisitos relativos à gestão segura dos dados e à subcontratação do tratamento de dados. A auditoria concluiu que os regulamentos internos das organizações de gestão de dados no que respeita a essas atividades de gestão tinham assegurado a proteção

dos recursos de dados nacionais enquanto ativos nacionais, em conformidade com as disposições jurídicas em vigor entre 2011 e 2015. Os responsáveis pelo tratamento dos dados tinham aplicado devidamente os requisitos, e as transferências de dados para terceiros tinham sido realizadas de forma adequada.

67 A **ISC da Polónia, *Najwyższa Izba Kontroli*,** avaliou a segurança dos dados recolhidos nos sistemas destinados a executar tarefas públicas importantes. A auditoria abrangeu seis instituições selecionadas que executavam tarefas públicas significativas. O grau de preparação e de aplicação do Sistema de Segurança da Informação não proporcionava um nível aceitável de segurança dos dados recolhidos nos sistemas informáticos utilizados para executar tarefas públicas importantes. Os processos de segurança da informação eram executados de forma desordenada e, dada a ausência de procedimentos, intuitiva. Entre as seis unidades auditadas, apenas uma tinha aplicado o Sistema de Segurança da Informação, embora deva notar-se que o funcionamento do sistema apresentava também falhas significativas. A auditoria concluiu que as recomendações e requisitos gerais relacionados com a segurança informática devem ser desenvolvidos e executados a nível central, sendo aplicáveis a todas as entidades públicas.

Análises da cibersegurança

68 O ***Tribunal de Contas Europeu*** analisou o panorama da política de cibersegurança da UE e assinalou os principais desafios à sua execução eficaz. Abrangeu a segurança das redes e das informações, a cibercriminalidade, a ciberdefesa e a desinformação. A análise do TCE detetou várias lacunas na legislação da UE em matéria de cibersegurança e constatou diferenças na transposição da legislação da UE pelos Estados-Membros. Por fim, a análise chamou a atenção para a falta de dados fiáveis sobre os ciberincidentes a nível da UE e para a inexistência de uma visão de conjunto das despesas da UE e dos seus Estados-Membros no domínio da cibersegurança. A análise constatou também que as agências da UE com responsabilidades na cibersegurança são afetadas por restrições de recursos, tendo, designadamente, dificuldades em atrair e reter talentos. Um outro desafio constatado dizia respeito ao desfasamento entre o financiamento da cibersegurança e os objetivos estratégicos da UE.

PARTE III – Resumo dos relatórios das ISC

Dinamarca
Rigsrevisionen

Proteção contra ataques de *ransomware*

Data de publicação: 2017

Hiperligação para o relatório: Resumo do relatório (versão em língua inglesa)

Tipo e período de auditoria

Tipo de auditoria: Auditoria de resultados

Período de auditoria: Abril-setembro de 2017

Resumo do relatório

Tema da auditoria

Este relatório verificou se determinadas instituições públicas essenciais dispunham de uma proteção satisfatória contra o *ransomware*.

As instituições públicas são alvos frequentes de ciberataques, e o *ransomware* é atualmente uma das maiores ameaças à cibersegurança. O *ransomware* é um *software* malicioso que bloqueia o acesso a dados. De um modo geral, encripta os dados e impede as instituições atacadas de os utilizar. Os *hackers* exigem um resgate para desencriptar os dados e permitir que as instituições voltem a poder aceder-lhes. O *ransomware* representa, portanto, uma grave ameaça à acessibilidade dos dados.

A impossibilidade súbita de aceder aos dados pode dificultar ou mesmo impedir totalmente a prestação de serviços importantes pelas instituições. As instituições afetadas por um ataque de *ransomware* são geralmente obrigadas a encerrar, total ou parcialmente, a sua rede informática para averiguar a dimensão do ataque. Os ataques de *ransomware* podem ter um impacto económico significativo, uma vez que as instituições estão sujeitas a quebras de atividade, por exemplo, se não puderem aceder à sua rede informática ou perderem dados que recolheram e trataram durante um longo período de tempo. Em 2017, um ataque de *ransomware* contra o serviço

nacional de saúde britânico levou ao cancelamento de 19 000 cirurgias e consultas. Por conseguinte, os órgãos de gestão das instituições devem estar atentos ao risco de ataques deste tipo e executar os controlos de segurança necessários para as proteger contra o *ransomware* e reduzir o impacto de um potencial ataque.

Este estudo incluiu a Autoridade dos Dados de Saúde, o Ministério dos Negócios Estrangeiros, a *Banedanmark* (rede ferroviária) e a Agência de Gestão de Emergências da Dinamarca. Estas quatro instituições foram selecionadas por serem responsáveis pela prestação de serviços essenciais na saúde, nos negócios estrangeiros, nos transportes e na preparação para emergências, domínios em que o acesso aos dados pode ter uma importância crítica. A Autoridade dos Dados de Saúde também presta serviços informáticos centralizados à maioria dos organismos públicos sob a alçada do Ministério da Saúde.

Este estudo tinha como objetivo avaliar se as quatro instituições dispunham de uma proteção satisfatória contra ataques de *ransomware* por correio eletrónico. Assim, a ISC examinou 20 controlos de segurança comuns que proporcionam uma proteção básica contra o *ransomware*. Além disso, analisou cinco controlos de segurança que as instituições devem ponderar no âmbito de futuras avaliações dos riscos. Os controlos virados para o futuro incluem, por exemplo, novas tecnologias que podem reduzir o número de mensagens de correio eletrónico falsas que entram numa instituição ou detetar atividades invulgares em computadores e emitir alertas em conformidade. A ISC deu início ao estudo com base nas constatações de quatro auditorias informáticas realizadas entre abril e setembro de 2017. O estudo apresenta uma visão global do nível de proteção das instituições contra o *ransomware*. As instituições em causa tiveram a oportunidade de aplicar os 20 controlos de segurança comuns após a conclusão das auditorias informáticas. Assim, os resultados do estudo dizem respeito apenas à proteção das instituições contra o *ransomware* à data da realização das quatro auditorias informáticas. O estudo contém uma apresentação do desempenho das quatro instituições, mas não inclui uma análise comparativa nem uma classificação desse desempenho.

Constatações e conclusões

Segundo a avaliação da ISC, as quatro instituições não dispunham de uma proteção satisfatória contra o *ransomware*. O estudo demonstra que as quatro instituições não tinham aplicado vários controlos de segurança comuns destinados a atenuar os ataques. Mais concretamente, a Autoridade dos Dados de Saúde e a *Banedanmark* apresentavam lacunas consideráveis na segurança. Assim, as quatro instituições

estavam expostas a um risco acrescido de ataques de *ransomware* por correio eletrónico que as impediriam de prestar os respetivos serviços durante períodos de tempo variáveis. As quatro instituições comunicaram à ISC que, após a conclusão do estudo, tinham procurado aplicar vários dos controlos de segurança referidos para aumentar o nível de proteção contra o *ransomware*.

A prevenção das instituições contra os ataques de *ransomware*, incluindo ameaças internas e externas, era inadequada. É especialmente preocupante que nenhuma das instituições tenha assegurado que os *patches* do *software* estavam atualizados e que três instituições não tenham aplicado listas de permissões para evitar que o seu pessoal executasse *malware*. Esta situação aumenta o risco de o *ransomware* infetar, total ou parcialmente, a rede informática e se propagar.

Em três destas instituições, os órgãos de gestão não prestaram atenção suficiente à ameaça de *ransomware* e as avaliações dos riscos realizadas pelos gestores na Autoridade dos Dados de Saúde e na *Banedanmark* não abrangiam todos os aspetos pertinentes. Como tal, as instituições não dispunham de uma avaliação atualizada da ameaça de *ransomware* e encontravam-se, por conseguinte, numa posição frágil para evitar novos ataques e reduzir o impacto de ataques futuros. Na Autoridade dos Dados de Saúde e na *Banedanmark*, os órgãos de gestão não tinham prestado atenção suficiente à avaliação dos riscos, pelo que a segurança informática destas duas instituições não se baseava em prioridades definidas pelos gestores.

Três das instituições não dispunham de planos adequados de resposta a incidentes que as ajudassem a restabelecer as suas atividades após um ataque de *ransomware*. É especialmente significativo que três das instituições não testassem regularmente a sua capacidade de repor os dados e os sistemas afetados por um ataque de *ransomware*. Esta situação aumenta o risco de as instituições perderem os dados que detêm devido a um ataque de *ransomware* e não conseguirem prestar os respetivos serviços durante um período de tempo mais longo.

Tendo em conta a constante mutação dos cenários de risco, é importante que as instituições ponderem introduzir controlos de segurança virados para o futuro, a fim de aumentar a sua resiliência a ataques de *ransomware*, ou seja, controlos que facilitem a verificação da identidade dos remetentes no correio eletrónico e que permitam detetar e filtrar mensagens de correio eletrónico que possam ser nocivas. As quatro instituições estão a desenvolver alguns destes controlos de segurança virados para o futuro, que as ajudarão a aumentar a sua proteção contra ataques de *ransomware*.

Outros relatórios no mesmo domínio

Título do relatório:	Relatório sobre a proteção dos dados da investigação nas universidades dinamarquesas
Hiperligação para o relatório:	Resumo do relatório (versão em língua inglesa)
Data de publicação:	2019

Título do relatório:	Relatório sobre a proteção dos sistemas informáticos e dos dados relativos à saúde em três regiões dinamarquesas
Hiperligação para o relatório:	Resumo do relatório (versão em língua inglesa)
Data de publicação:	2017

Título do relatório:	Relatório sobre a gestão da segurança informática dos sistemas externalizados a fornecedores externos
Hiperligação para o relatório:	Resumo do relatório (versão em língua inglesa)
Data de publicação:	2016

Título do relatório:	Relatório sobre o acesso aos sistemas informáticos que apoiam a prestação de serviços essenciais à sociedade dinamarquesa
Hiperligação para o relatório:	Resumo do relatório (versão em língua inglesa)
Data de publicação:	2015

Estónia
Riigikontroll

Garantir a segurança e a preservação de bases de dados estatais de importância crítica na Estónia

Data de publicação: Maio de 2018

Hiperligação para o relatório: Resumo do relatório (versão em língua inglesa)
Relatório (versão em língua estónia)

Tipo e período de auditoria

Tipo de auditoria: Auditoria de resultados

Período de auditoria: 2017

Resumo do relatório

Tema da auditoria

A preservação da independência estónia exige não apenas a defesa física do território, mas também a proteção dos ativos digitais de importância primordial para o Estado contra os eventos que representam as maiores ameaças. Os ativos digitais que mais necessitam de proteção são os dados relativos aos cidadãos, ao território e à legislação. No entanto, é necessário proteger também os dados referentes à propriedade, aos bens imóveis e aos direitos das pessoas residentes na Estónia.

A ISC verificou a forma como o Estado determinava quais os dados e as bases de dados que considerava cruciais para garantir a segurança nacional. Verificou igualmente a proteção da segurança e a continuidade destes dados e bases de dados, apresentando uma síntese das ferramentas utilizadas para proteção.

A segurança física da Estónia está mais garantida após a sua adesão à NATO e à União Europeia. Contudo, a Estónia tem de analisar a possibilidade de ciberameaças em caso de agravamento dos problemas de segurança. Estes cenários de risco, conjugados com um aumento do número de incidentes relacionados com a segurança da informação, nomeadamente ciberataques e fugas de dados, poderão também comprometer os

dados e as bases de dados mais importantes para o Estado. Se os dados de importância primordial para o Estado fossem alterados sem autorização, divulgados ou perdidos, o Estado deixaria de conseguir exercer funções necessárias, nomeadamente garantir a proteção da segurança das pessoas, satisfazer necessidades, criar o ambiente necessário à atividade empresarial e muitas outras. A Estónia prevê despender inicialmente cerca de um milhão de euros no armazenamento de dados de importância crítica no estrangeiro.

Questões de auditoria

- Os ministérios identificaram todas as bases de dados de importância crítica e os requisitos de tratamento?
- As bases de dados e os registos de importância crítica estão protegidos?
- A continuidade a longo prazo dos dados e bases de dados de importância crítica está assegurada?

Constatações

A ISC formulou as observações que se seguem acerca das bases de dados de importância crítica auditadas.

- Não tinham sido estabelecidos planos de ação ou requisitos para a aplicação do conceito de bases de dados de importância crítica. As condições de seleção das bases de dados não tinham sido determinadas, e nada garantia que todas as bases de dados necessárias tivessem sido incluídas no processo. A proteção adicional das bases de dados tinha sido organizada informalmente e não era obrigatória para os proprietários das bases de dados, razão pela qual os dados das cinco bases de dados de importância crítica não tinham cópias de segurança no estrangeiro.
- Não tinham sido estabelecidas regras adicionais de segurança da informação nas bases de dados de importância crítica. Nem o sistema de segurança da informação ISKE (uma norma de segurança da informação desenvolvida para o setor público da Estónia que é obrigatória para as organizações da administração nacional e local que trabalham com bases de dados ou registos), nem qualquer norma ou ato jurídico incluíam requisitos adicionais para as bases de dados de importância crítica, como cópias de segurança dos dados fora da Estónia. Algumas cópias de segurança das bases de dados auditadas foram colocadas no

estrangeiro, mas a recuperação do trabalho dos sistemas de informação a partir dessas cópias não tinha sido testada.

- A aplicação do ISKE e as auditorias associadas constituíam um problema relativamente às bases de dados de importância crítica. À data da auditoria, o ISKE não tinha sido auditado no que respeita a duas das 10 bases de dados, e as auditorias efetivamente realizadas apenas tinham sido organizadas no final da auditoria nacional (30 de novembro de 2017). Apenas duas bases de dados de importância crítica tinham sido auditadas com a frequência exigida por lei. Além disso, em alguns casos, os problemas assinalados pelo auditor não tinham sido corrigidos durante o período compreendido entre as duas auditorias do ISKE (dois a três anos).

- Durante a sua auditoria, a ISC constatou que certas medidas importantes de segurança da informação não tinham sido aplicadas em algumas bases de dados de importância crítica. Por exemplo, não tinham sido definidos requisitos de avaliação regular das vulnerabilidades dos sistemas de informação em orientações sobre a segurança da informação, não tinham sido realizadas verificações ou análises regulares de ficheiros de registo de ocorrências, não existiam planos de formação em segurança da informação nem análises da sensibilização para este aspeto no setor da administração que elabora os planos de formação, não houve, em alguns casos, uma verificação da integridade dos ficheiros e não foram realizados testes de penetração externa.

Conclusões e recomendações

A auditoria revelou que, apesar da aplicação do ISKE, um sistema de segurança de base em três níveis, cuja utilização é obrigatória nos organismos públicos e nas suas auditorias, existiam insuficiências significativas na garantia da segurança da informação em várias bases de dados cruciais, como a análise de ficheiros de registo, os testes de penetração e a proteção de dispositivos móveis. Os requisitos especiais necessários para proteger dados de importância crítica ainda não tinham sido estabelecidos.

O Ministério dos Assuntos Económicos e das Comunicações tinha lançado as primeiras atividades necessárias para proteger esses dados, mas o projeto das bases de dados de importância crítica encontrava-se numa fase que exigia um conjunto de regras juridicamente vinculativas. Além disso, não existia uma análise pormenorizada dos riscos nem um plano de ação para o futuro.

As cópias de segurança de cinco bases de dados de importância crítica encontravam-se em embaixadas em países estrangeiros, mas, caso ocorresse uma destruição física dos centros de dados situados na Estónia, a preservação dos dados de importância crítica nas restantes cinco bases de dados não estaria garantida.

A auditoria formulou duas recomendações gerais:

- determinar as regras para proteção adicional das bases de dados de importância crítica, incluindo a seleção destas bases de dados, o tratamento de dados neste contexto e as cópias de segurança dos dados de importância crítica para o Estado, e avaliar formas de disponibilizar financiamento adicional para estas atividades;
- analisar as diferentes fases da criação das bases de dados, tanto em termos de planeamento do financiamento como de segurança da informação, e aplicar as melhores práticas de gestão de projetos na execução destas fases.

Irlanda
Office of the Comptroller and Auditor General

Medidas relacionadas com a cibersegurança nacional

Data de publicação: Setembro de 2018

Hiperligação para o relatório: Resumo do relatório (versão em língua inglesa)

Tipo e período de auditoria

Tipo de auditoria: Auditoria de resultados

Período de auditoria: 2011-2018

Resumo do relatório

Tema da auditoria

O Ministério das Comunicações, da Ação Climática e do Ambiente é responsável pela política de cibersegurança na Irlanda, bem como, através do Centro Nacional de Cibersegurança, pela coordenação da resposta de emergência do Estado a quaisquer incidentes de cibersegurança a nível nacional.

O Centro Nacional de Cibersegurança foi criado em 2011. Este centro tem como principais objetivos proteger as redes públicas, ajudar as empresas e as pessoas a protegerem os seus próprios sistemas e salvaguardar infraestruturas nacionais de importância crítica.

Questões de auditoria

Este exame analisa os progressos realizados nas medidas de cibersegurança após a criação do Centro Nacional de Cibersegurança, incidindo, em especial, em questões relacionadas com:

- o mandato do Centro e os recursos que lhe são atribuídos;

- a Estratégia Nacional de Cibersegurança (2015-2017);
- a aplicação da Diretiva Segurança das Redes e da Informação da UE;
- os mecanismos de governação e supervisão.

Constatações e conclusões

A decisão governamental relativa à criação do Centro Nacional de Cibersegurança aprovou um financiamento anual de 800 000 euros, mas o financiamento anual real destinado à cibersegurança, entre 2012 e 2015, foi inferior a um terço desse montante. Em 2017, a dotação aumentou para 1,95 milhões de euros. Os efetivos do centro quase duplicaram em 2017, para 14,5 equivalentes a tempo completo. Em 2018, foi concedida aprovação para a nomeação de mais 16 efetivos.

A Estratégia Nacional de Cibersegurança (2015-2017) estabeleceu 12 medidas a concretizar ao longo do período da estratégia. Em maio de 2018, quatro medidas tinham sido concluídas, quatro tinham sido parcialmente executadas e quatro não tinham sido executadas.

A Diretiva Segurança das Redes e da Informação da UE visa melhorar a resiliência de redes e sistemas de informação essenciais. A avaliação dos progressos realizados na Irlanda relativamente a cada um dos três pilares previstos na diretiva concluiu o seguinte:

- *Pilar 1 – Melhorar as capacidades dos Estados-Membros da UE no domínio da cibersegurança:* parcialmente executado – os requisitos estruturais foram abordados, mas subsistem lacunas no planeamento estratégico;
- *Pilar 2 – Facilitar a cooperação entre os Estados-Membros da UE no domínio da cibersegurança:* executado;
- *Pilar 3 – Introduzir medidas de segurança e obrigações de comunicação de incidentes para setores essenciais:* parcialmente executado – ainda há trabalho a fazer no que diz respeito à identificação das redes e sistemas de informação de importância crítica, à designação formal de entidades como operadoras de serviços essenciais e à gestão dos prestadores de serviços digitais.

A decisão governamental (julho de 2011) que aprovou a criação do Centro Nacional de Cibersegurança aprovou também a criação de um comité interministerial destinado a criar e aplicar políticas para dar resposta aos desafios da cibersegurança na Irlanda.

Embora este grupo se tenha reunido cinco vezes entre 2013 e 2015, apenas estava disponível para análise a ata de uma reunião. O comité não se reúne desde 2015.

O Plano de Execução da Estratégia Nacional de Cibersegurança previa a publicação de um relatório anual e a realização de uma avaliação de impacto formal do trabalho do comité no final de 2017. Estas ações continuam pendentes, apesar de as atividades do centro se encontrarem descritas no relatório anual do ministério.

O ministério solicitou formalmente uma avaliação do desempenho do centro, mas não foram apresentadas provas da realização desta avaliação. O ministério afirmou que a avaliação dos resultados do trabalho do Centro Nacional de Cibersegurança fazia parte das suas atividades normais em matéria de gestão do desempenho e governação institucional.

A auditoria conclui o seguinte:

- embora o Centro Nacional de Cibersegurança desempenhe uma função crucial, o nível dos recursos que lhe foram atribuídos nos primeiros quatro anos de funcionamento foi significativamente inferior ao inicialmente previsto;
- a orientação estratégica global do Centro não é clara e não existe qualquer plano estratégico atualmente em vigor;
- é necessária maior clareza quanto aos papéis específicos dos organismos envolvidos na investigação dos cibercrimes e dos incidentes de segurança nacional;
- ainda não foram aplicados os requisitos da Diretiva Segurança das Redes e da Informação da UE relativos à elaboração de uma estratégia nacional;
- apesar de terem sido estabelecidas estruturas de governação, não é claro como funcionam, na prática, os mecanismos de governação.

Falta transparência no que respeita à disponibilidade e ao custo dos recursos dedicados à cibersegurança.

França
Cour des comptes

Acesso ao ensino superior: uma avaliação inicial da Lei relativa à orientação e ao sucesso dos estudantes

Data de publicação: Fevereiro de 2020

Hiperligação para o relatório: Relatório (versão em língua francesa)

Tipo e período de auditoria

Tipo de auditoria: Auditoria de resultados

Período de auditoria: 2019-2020

Resumo do relatório

Tema da auditoria

O objetivo da Lei relativa à orientação e ao sucesso dos estudantes (*loi relative à l'orientation et à la réussite des étudiants*, ORE), de 2018, consistia em melhorar as três principais fases do percurso seguido pelos estudantes no acesso ao ensino superior: orientação e apoio para os estudantes do ensino secundário, seleção dos cursos e sucesso nos primeiros anos de estudo. A referida lei introduziu a *Parcoursup*, uma nova plataforma digital que constitui uma fonte de informação sobre os cursos disponíveis e os requisitos de acesso, tendo como objetivo aumentar a correspondência entre as aptidões e os resultados académicos dos estudantes do ensino secundário e os conteúdos dos cursos de ensino superior.

Os dois primeiros anos da ORE constituíram um primeiro passo para transformar o acesso ao ensino superior. Apesar das muitas limitações existentes, a implantação da *Parcoursup* decorreu de forma harmoniosa, mas continuavam a faltar garantias de segurança e sustentabilidade e um melhor aproveitamento dos dados, tendo em conta a sua importância.

A ORE foi adotada para resolver dois grandes problemas na política educativa. O primeiro dizia respeito à elevada taxa de abandono dos estudantes universitários. O segundo era a insatisfação profunda provocada pelo facto de a anterior plataforma digital utilizar uma seleção aleatória na fase final.

A reforma da ORE recebeu financiamento de 867 milhões de euros ao longo de cinco anos. Tinha por base um conceito de continuidade "-3/+3", assente no princípio de que, quanto maior fosse o conhecimento dos estudantes do ensino secundário sobre os conteúdos dos cursos de ensino superior, maiores seriam as suas hipóteses de sucesso nos exames, uma vez que escolheriam os cursos mais adequados às suas aptidões e ambições. A ORE procurava colmatar a falta de orientações disponíveis para os estudantes do ensino secundário e, dessa forma, reduzir as mudanças de cursos, que, segundo as estimativas da ISC, implicavam custos de quase 550 milhões de euros por ano relativamente apenas ao primeiro ano do ensino superior.

Os auditores realizaram uma avaliação inicial do acesso ao ensino superior no contexto da ORE, analisando as questões de segurança informática suscitadas pela plataforma.

O sistema de informação caracterizava-se por uma expansão dos fatores de carregamento (inclusão, em 2020, de todos os cursos de ensino superior e um rápido aumento do número de utilizadores em apenas alguns anos). Esta situação refletiu a mudança apressada da anterior plataforma para a *Parcoursup* sem uma alteração da arquitetura, criando assim riscos significativos em termos de qualidade, continuidade, adaptabilidade e desenvolvimento futuro do serviço. As insuficiências do sistema relativamente à segurança, ao desempenho e à robustez não tinham sido corrigidas. Foi possível criar a *Parcoursup* rapidamente porque esta era gerida em modo beta por um grupo restrito de pessoas altamente qualificadas e motivadas, mas, devido a esta abordagem, o mecanismo não possuía uma orientação estratégica nem uma governação satisfatória.

Os auditores avaliaram a qualidade do sistema de informação e o desempenho da nova plataforma *Parcoursup*, criada ao abrigo da ORE com o objetivo de melhorar a qualidade da correspondência com os cursos de ensino superior e, assim, impulsionar a taxa de conclusão de estudos.

Constatações

Embora a *Parcoursup* funcionasse de forma satisfatória, estava exposta a riscos informáticos que tinham de ser reduzidos. Eram necessárias garantias relativas à segurança e à sustentabilidade da plataforma e os dados poderiam ter sido mais utilizados.

Um sistema de informação antigo

Existiam poucos elementos novos na *Parcoursup*, que herdou a rigidez e a fragilidade da anterior plataforma *Admission Post-Bac* (APB), bem como muitos dos seus riscos não resolvidos. O sistema de informação que constituía a base estrutural da *Parcoursup* foi retirado diretamente da plataforma anterior. Apesar de a plataforma ser anunciada como uma nova ferramenta de correspondência, o núcleo do sistema de informação tinha sido apenas ligeiramente alterado em relação à APB. Com efeito, 72% da infraestrutura de informação permaneciam inalterados, já que menos de 30% do código da APB tinha sido reescrito.

A base informática da plataforma foi concebida no início da década de 2000 para tratar cerca de um milhão de candidaturas para aproximadamente 100 000 lugares por ano, mas o âmbito do sistema de informação foi alargado de modo a tratar um fluxo anual de cerca de 10 milhões de candidaturas para aproximadamente um milhão de lugares. A *Parcoursup* era vista como uma ferramenta antiga com uma nova marca. O aumento do volume suscitou questões sobre a capacidade da plataforma para cumprir a sua finalidade.

Um sistema de informação mal documentado

Apesar dos esforços de transparência do ministério, 99% do código-fonte da *Parcoursup* continuou fechado. A pequena parte publicada tinha um interesse limitado em termos de compreensão, análise e avaliação do processo de correspondência dos candidatos aos cursos.

Tal como a sua antecessora, a *Parcoursup* era um sistema de informação operacional mal documentado. Os resultados da auditoria do código indicaram que a aplicação apresentava uma qualidade baixa e riscos elevados, tendo sido identificadas muitas violações importantes. Este sistema tinha uma qualidade inferior à de outros programas informáticos com uma idade semelhante, apresentando um elevado risco de falhas anormais.

A *Parcoursup* utilizava simultaneamente código-fonte público e fechado. O código aberto apresentava uma taxa muito maior de violações importantes do que o código fechado, criando riscos de perturbação do serviço. A plataforma também não estava protegida contra *hackers* (auditoria da segurança do código-fonte, de julho de 2018). Contudo, no final de 2019, o ministério anunciou que tinha iniciado um procedimento de certificação relativo ao código da *Parcoursup*.

A documentação disponível sobre o código-fonte não era coerente nem exaustiva. O código da *Parcoursup* era excecionalmente complexo. Os auditores referiram que o código-fonte deveria ser reestruturado para reduzir o número de componentes complexos.

O sistema de informação da *Parcoursup* tinha uma arquitetura de alto risco; a base de dados era gerida de forma arcaica, ou seja, manualmente. A fragilidade do sistema residia na sua elevada dependência da disponibilidade e da vigilância de um operador. O ministério reconheceu que a arquitetura da *Parcoursup* estava associada a riscos elevados, que não podiam ser corrigidos sem um desenvolvimento adicional da aplicação.

O sistema de informação da *Parcoursup* estava mal documentado, baseando-se essencialmente no conhecimento especializado do pessoal do organismo público nacional competente (*Service à Compétence Nationale*, SCN). A documentação consistia em observações escritas na base de dados no núcleo do sistema, sendo assim difícil manter e desenvolver o sistema de informação e explorar os dados. Não era fácil extrair e avaliar as informações dos utilizadores conservadas na plataforma sem uma investigação aprofundada. Dada a falta de documentação técnica estruturada, a capacidade do SCN para cumprir as suas tarefas estratégicas estava totalmente dependente do diretor do centro de informática.

Necessidade de melhorar a estratégia de segurança

Devido à natureza sensível dos dados pessoais contidos no sistema, a *Parcoursup* representa um verdadeiro desafio de segurança. Em princípio, todas as organizações que gerem um sistema de informação devem dispor de uma política de segurança dos sistemas de informação (PSSI) formal e escrita. Apesar de reconhecida pelo Primeiro-Ministro como um prestador de serviços essenciais, a *Parcoursup* não tinha uma PSSI, pelo que eram necessárias medidas imediatas para introduzir uma política deste tipo.

Cada equipa da *Parcoursup* dispunha de um responsável pela segurança dos sistemas de informação (RSSI) afetado ao centro de informática. Teria constituído uma boa prática colocar os RSSI sob a alçada direta do diretor do SCN para garantir a sua independência.

Em meados de 2019, ainda se procurava garantir a conformidade da *Parcoursup* com o RGPD. Algumas medidas estavam ainda pendentes, em especial a necessidade de instituir formalmente os vários procedimentos utilizados no tratamento de dados. A segurança dos dados pessoais permanecia inadequada, e continuavam a ser conservados demasiados dados individuais exaustivos.

A unidade *Parcoursup* respondia perante o gestor do projeto *Parcoursup*, designado no gabinete do ministro, e perante o Serviço da Estratégia de Formação e dos Assuntos dos Estudantes inserido na Direção-Geral do Ensino Superior e da Inserção Profissional, estando por isso sujeita a conflitos de interesses. As questões práticas relacionadas com o sistema de informação da *Parcoursup* eram tratadas em reuniões semanais. Esta forma de organização permitia reações rápidas na gestão quotidiana dos fluxos de estudantes, mas deixava a *Parcoursup* estrategicamente à deriva.

Por último, o sistema não era suficientemente transparente, nem permitia a melhor utilização dos dados conservados na plataforma, apesar do seu enorme potencial. O aproveitamento deste potencial teria certamente proporcionado melhorias de desempenho.

Conclusões e recomendações

O Governo conseguiu centralizar o acesso aos estudos pós-secundários através de uma plataforma digital, combinando todos os programas educativos, para fazer face à generalização do ensino superior. O sistema anterior foi apressadamente reformulado na *Parcoursup*, sem alterações estruturais substantivas. Por conseguinte, as vulnerabilidades do sistema de informação em termos de segurança, desempenho e robustez ficaram por resolver, apesar de ser previsível que a carga continuaria a aumentar devido ao objetivo último de incluir todos os cursos de licenciatura. Além disso, o sistema estava mal documentado, devido a uma abordagem algo rudimentar do desenvolvimento informático, e a sua invulgar complexidade aumentava os riscos de erro em caso de alterações operacionais. A plataforma continuava, portanto, sujeita a riscos significativos em termos de qualidade e continuidade do serviço público e de segurança dos dados pessoais.

A ISC formulou as seguintes recomendações:

- a equipa informática do SCN deve ter mais efetivos e o financiamento no âmbito da ORE deve ser reafetado de modo a reforçar os recursos humanos e financeiros da subdireção responsável pelos sistemas de informação e pela investigação estatística;
- o sistema de informação deve ser estabelecido numa perspetiva de longo prazo, corrigindo as suas falhas mais urgentes, modernizando ou reestruturando a sua arquitetura e documentando as bases de dados principais tanto do sistema antigo como da *Parcoursup* de uma forma sistemática e estruturada;
- o sistema de informação da *Parcoursup* deve dispor de uma política de segurança;
- deve ser criado um órgão diretor para o Ministério da Educação e Juventude e o Ministério do Ensino Superior, Investigação e Inovação, incumbido de supervisionar a plataforma *Parcoursup*, com recursos reafetados do financiamento no âmbito da ORE destinado a atividades de "orientação".

Letónia
Valsts Kontrole

A administração pública aproveitou todas as oportunidades para uma gestão eficiente das infraestruturas das TIC?

Data de publicação: Junho de 2019

Hiperligação para o relatório: Resumo do relatório (versão em língua inglesa)

Tipo e período de auditoria

Tipo de auditoria: Auditoria de resultados

Período de auditoria: 2017-2019

Resumo do relatório:

Tema da auditoria

A ISC da Letónia concluiu uma auditoria de resultados relativa à eficiência das infraestruturas públicas das TIC. A auditoria tinha como objetivo verificar se a administração pública possuía uma abordagem unificada para uma gestão eficiente das infraestruturas das TIC e se as instituições tinham avaliado os benefícios da centralização. Além disso, a segurança dos centros de dados foi apontada como uma questão importante na avaliação de opções para otimizar o planeamento.

Devido à relutância das autoridades em gerir centralmente as infraestruturas das TIC, pelo menos ao nível de um ministério, tinham sido criadas várias salas de servidores, que aumentaram significativamente os custos de manutenção. Nos quatro ministérios auditados, existiam 22 subentidades que utilizavam 38 centros de dados. Durante a auditoria, a ISC observou situações em que sistemas de informação de importância significativa, ou mesmo de importância nacional, estavam localizados em instalações com um nível de segurança insuficiente. A otimização do número de salas de servidores permitiria não apenas reduzir as despesas com as TIC, mas também proporcionar um nível de segurança suficiente a um custo mais baixo. Entretanto, já

existiam nas instituições salas de servidores de alta segurança, mas estas não eram plenamente aproveitadas.

Principal tema da auditoria

A auditoria tinha como objetivo verificar se todos os elementos essenciais para a gestão unificada das infraestruturas das TIC tinham sido criados e eram aplicados de forma a promover uma utilização mais eficiente e segura dos recursos das TIC.

Constatações e conclusões

Governação e otimização das TIC

- Não existia, a nível nacional ou nos ministérios, uma visão de longo prazo do desenvolvimento e da otimização das TIC. Os ministérios e as respetivas subentidades otimizavam as infraestruturas das TIC de acordo com o seu conhecimento e a sua capacidade.

Entre 2011 e 2017, os custos totais de manutenção das TIC nas instituições auditadas aumentaram de 17 para 20 milhões de euros por ano. Não tinha sido introduzida nas instituições qualquer prática de avaliação regular da opção mais económica entre assegurar internamente a manutenção das infraestruturas das TIC, cooperar com outra instituição ou subcontratar a manutenção das TIC. A centralização ou a descentralização das TIC não constituem objetivos em si, sendo necessária uma análise da situação concreta e das alternativas para proporcionar clareza quanto aos custos atuais e às possíveis alternativas.

Segurança das TIC

- O quadro jurídico não definia claramente os requisitos de segurança das infraestruturas das TIC num sistema lógico em função da relevância das informações a tratar. Não existiam requisitos técnicos pormenorizados para a proteção dos centros de dados das TIC.

- Devido às insuficiências nos requisitos de segurança, a proteção era dispendiosa ou, pelo contrário, não estava assegurada a proteção das informações de importância nacional. Alguns sistemas de informação importantes estavam, inclusivamente, alojados em centros de dados de baixa segurança.

- Existiam ameaças de segurança na maior parte das salas de servidores, já que os centros de dados não estavam suficientemente protegidos contra o acesso físico e os riscos ambientais. Para prevenir as ameaças de segurança, eram necessários pelo menos 247 000 a 765 000 euros, consoante a abordagem escolhida, nomeadamente: 1) melhorar as salas de servidores que continham sistemas de informação mais importantes e assegurar o armazenamento de recursos significativos das TIC em centros de dados mais seguros; ou 2) melhorar todas as salas de servidores existentes. Esta opção exigiria, contudo, um montante de investimento que os auditores apenas considerariam justificado se o número de centros de dados fosse minimizado.

O quadro jurídico estava incompleto, uma vez que não existiam requisitos de segurança pormenorizados para as infraestruturas das TIC. Por exemplo, existiam requisitos para vários critérios relacionados com a segurança lógica, mas não existiam critérios relativos à segurança física e ambiental das infraestruturas, que também afeta a disponibilidade dos sistemas e a proteção dos dados. Embora os documentos de planeamento da política pública salientassem a importância da segurança das infraestruturas das TIC e a necessidade de a reforçar, nenhuma entidade tinha programado atividades específicas neste domínio. Dada a ausência de uma diferenciação clara, rastreável e lógica dos requisitos de segurança, existia o risco de os requisitos de segurança para tratar informações de igual importância e relevância variarem em diferentes pontos do país.

A segurança no espaço digital era acompanhada centralmente pelo Estado, que respondia aos incidentes nesse domínio, mas a responsabilidade pela aplicação da segurança das infraestruturas informáticas cabia ao diretor de cada instituição. Por conseguinte, a interpretação das questões de segurança das TIC pelas instituições, a avaliação da importância das informações tratadas e os recursos de que as instituições dispunham para resolver as questões de segurança das TIC variavam consideravelmente.

Era necessário um sistema de acompanhamento regular para estes processos, a fim de avaliar toda a administração pública como um sistema único, de forma independente e com critérios normalizados, de identificar diferentes abordagens e evitar problemas assinalando riscos comuns e de planear ações preventivas para atenuar estes riscos.

Lituânia
Valstybės Kontrolė

Gestão dos recursos de informação de importância crítica do Estado

Data de publicação: Junho de 2018

Hiperligação para o relatório: Resumo do relatório (versão em língua inglesa)
Relatório (versão em língua lituana)

Tipo e período de auditoria

Tipo de auditoria: Auditoria de resultados

Período de auditoria: 2014-2017

Resumo do relatório

Tema da auditoria

A utilização dos recursos de informação de importância crítica do Estado – informações eletrónicas de importância crítica – está associada ao cumprimento de funções públicas importantes, como a gestão das finanças públicas, a administração fiscal e os cuidados de saúde. Qualquer perda de informações de importância crítica ou indisponibilidade dos sistemas de informação correspondentes pode ter consequências graves para a segurança pública, o bem-estar e a economia. As avaliações do controlo informático geral realizadas pela ISC da Lituânia entre 2006 e 2016 revelaram problemas recorrentes na gestão informática (planeamento, definição da arquitetura de informação, estrutura organizacional, alterações, garantia da continuidade das atividades, segurança dos dados, acompanhamento e avaliação da gestão informática). A ISC realizou uma auditoria dos recursos de informação de importância crítica do Estado para avaliar a gestão e a segurança destes recursos e definir medidas de aperfeiçoamento.

A auditoria tinha como objetivo avaliar a gestão (controlo geral) e a maturidade dos recursos de informação de importância crítica do Estado e detetar problemas sistémicos.

A ISC avaliou a maturidade da gestão informática em 12 organizações do setor público[64] que geriam 44 sistemas de informação de nível um do Estado. A auditoria foi realizada de acordo com os Requisitos de Auditoria Pública e as Normas Internacionais das Instituições Superiores de Controlo. A avaliação foi realizada em conformidade com a metodologia COBIT[65] nos seguintes domínios de maior risco: planeamento informático estratégico; definição da arquitetura de informação; gestão dos riscos informáticos; gestão de alterações; garantia de prestação ininterrupta dos serviços; segurança dos sistemas; gestão dos dados; acompanhamento e avaliação das atividades informáticas; garantia da gestão informática. A avaliação do processo incluía a gestão informática tanto a nível organizacional como nacional e a interação entres estes níveis de gestão.

Constatações da auditoria

As tendências de evolução do nível de maturidade na gestão dos recursos de informação de importância crítica do Estado eram positivas. Contudo, tendo em conta o nível crescente das ciberameaças, os progressos observados eram demasiado lentos; por conseguinte, era necessário aumentar a segurança destes recursos, devido, em especial, às insuficiências a seguir descritas.

- A eficácia do sistema de identificação dos recursos de informação de importância crítica do Estado não era suficiente para permitir a aplicação de soluções de segurança que respondessem às necessidades reais:

  — as avaliações destinadas a comprovar a importância crítica dos recursos de informação do Estado eram pouco objetivas, as alterações nem sempre eram consideradas nas reavaliações, este processo não era acompanhado a nível nacional e as orientações para determinar a importância crítica não asseguravam uma execução eficaz;

---

[64] Inspeção Fiscal do Estado, empresa estatal Centro de Registos, Departamento das Tecnologias da Informação e da Comunicação, Conselho do Fundo Nacional da Segurança Social, empresa estatal Centro de Informação Agrícola e Economia Rural, Centro do Sistema de Informação Aduaneiro, Serviço Estatal da Alimentação e dos Produtos Veterinários, Gabinete do Parlamento (*Seimas*) da República da Lituânia, Ministério das Finanças, Comissão do Desenvolvimento da Sociedade da Informação, Fundo Nacional de Doença, Serviço Nacional das Florestas.

[65] COBIT (*Control Objectives for Information and Related Technology*) é uma norma da organização internacional ISACA que estabelece boas práticas de gestão informática.

— o sistema para identificação dos recursos e infraestruturas de informação de importância crítica do Estado não era normalizado; os recursos e as infraestruturas eram identificados de diferentes formas com base na importância da informação e dos serviços, complicando o processo de identificação destes recursos;

— não tinha sido desenvolvida uma arquitetura de informação nacional para representar os sistemas de informação do Estado e as suas interligações, demonstrar a escala dos recursos de informação de importância crítica do Estado e permitir tomar decisões fundamentadas sobre a importância dos mesmos.

o A gestão dos recursos de informação do Estado teria de estar mais harmonizada com as boas práticas e normas de gestão informática, a fim de alcançar a melhoria integrada do domínio da informática que contribuiria para melhores progressos na gestão dos recursos de informação de importância crítica do Estado:

— o planeamento informático não era sustentável: as ferramentas informáticas planeadas eram apresentadas em diferentes documentos e o excesso de documentos estratégicos impedia qualquer abordagem sistemática, tornando difícil identificar as principais prioridades e orientar os recursos para a gestão das maiores ameaças;

— o acompanhamento informático não garantia que as organizações medissem a eficiência das operações informáticas e que as auditorias realizadas pelos gestores dos recursos de informação de importância crítica do Estado revelassem a maturidade real da gestão informática. A gestão informática estatal não era controlada a nível nacional e as questões de gestão informática não eram sistematicamente analisadas. Tinha sido criado um sistema para acompanhar a conformidade dos recursos de informação do Estado com os requisitos da segurança das informações eletrónicas, destinado unicamente a facilitar o acompanhamento do cumprimento das regras de segurança, mas as funcionalidades desse sistema não eram suficientemente utilizadas.

o As medidas destinadas a assegurar a resiliência dos recursos de informação de importância crítica ao nível das ciberameaças não eram suficientemente eficazes; subsistia, por conseguinte, o risco de vulnerabilidade destes recursos:

— a eficácia da avaliação dos riscos de segurança informática tinha de ser aumentada, uma vez que nem todos os riscos pertinentes eram identificados e que a metodologia da sua avaliação não cumpria as práticas mais recentes de gestão informática; não era assegurada uma gestão oportuna dos riscos inaceitáveis;

— as medidas de segurança organizacionais suscetíveis de reduzir as ciberameaças não eram utilizadas de forma sistemática. Testes de segurança insuficientes, formação incompleta do pessoal durante o desenvolvimento, a atualização e a modificação do sistema de informação; ausência de gestão das configurações e atualizações para um software seguro; a gestão inadequada da continuidade das atividades informáticas e dos ficheiros das cópias de segurança punha em causa a recuperação da atividade; as medições do desempenho de segurança eram insuficientes e não contribuíam para o reforço da segurança.

Conclusões

Em média, a gestão informática pelas entidades do setor público auditadas nos últimos dez anos tinha alcançado o primeiro dos cinco[66] níveis de maturidade, situando-se num nível de 1,7 à data da elaboração do relatório. Este baixo nível de maturidade dos recursos de informação de importância crítica do Estado refletia insuficiências na elaboração e na execução da política relativa aos recursos de informação do Estado, que tornavam esses recursos mais vulneráveis. Para aumentar a segurança destes recursos, é necessário melhorar o mecanismo de gestão dos recursos de informação do Estado, de forma a corresponder o mais possível às boas práticas. Os auditores observaram também que as medidas para garantir a resistência dos recursos de informação de importância crítica às ciberameaças não eram suficientemente eficazes. Por conseguinte, é necessário aumentar a eficácia da avaliação dos riscos de segurança informática, colocando maior ênfase nos testes de segurança durante a criação e a modernização dos sistemas de informação e a formação do pessoal.

[66] Seguindo a metodologia COBIT.

Outros relatórios no mesmo domínio

Título do relatório:	A cibercriminalidade é combatida com eficácia?
Hiperligação para o relatório:	Resumo do relatório (versão em língua inglesa) Relatório (versão em língua lituana)
Data de publicação:	2020

Título do relatório:	O ambiente de cibersegurança na Lituânia
Hiperligação para o relatório:	Resumo do relatório (versão em língua inglesa) Relatório (versão em língua lituana)
Data de publicação:	2015

Hungria
Instituição Superior de Controlo

Auditoria relativa à proteção de dados – Auditoria do quadro nacional de proteção de dados e alguns registos de dados prioritários no âmbito da cooperação internacional

Data de publicação: Março de 2017

Hiperligação para o relatório: Relatório (versão em língua húngara)

Tipo e período de auditoria

Tipo de auditoria: Conformidade

Período de auditoria: 2011-2015

Resumo do relatório

Tema da auditoria

A segurança dos recursos de dados nacionais constitui um interesse fundamental da sociedade em todos os países tendo em vista a preservação e a proteção dos valores nacionais. Assim, garantir um reforço da segurança dos dados pessoais e públicos nos recursos de dados nacionais da Hungria é essencial para reforçar a confiança dos cidadãos no Estado e assegurar um funcionamento contínuo e harmonioso da administração pública. Consequentemente, a proteção de dados e a rede de segurança garantida pelo quadro jurídico relativo à sua aplicação são elementos de importância crucial para a sociedade.

No domínio da proteção de dados, a administração pública desempenha um papel fundamental na gestão dos registos de dados maiores e mais sensíveis pertencentes aos recursos de dados nacionais. Os responsáveis pelo tratamento dos dados nos registos cooperam de forma estreita no exercício das suas funções. Transferem regularmente registos com grandes quantidades de dados e têm de estar atentos aos requisitos jurídicos de proteção de dados. A utilização de sistemas de informação eletrónicos para gerir e tratar dados é essencial nos dias de hoje, pelo que é necessário

garantir, através de controlos devidamente concebidos e utilizados, uma operação adequada e fiável dos sistemas.

Durante as suas auditorias, a ISC da Hungria coloca especial ênfase na proteção de dados. Realizou auditorias exaustivas neste domínio entre 2011 e 2015 e publicou um relatório no primeiro trimestre de 2017. A auditoria em questão abrangeu também aspetos de auditorias internacionais, realizadas paralelamente em cooperação com o grupo de trabalho da EUROSAI sobre a informática, dedicadas principalmente ao cumprimento das diretivas em vigor da União Europeia.

A finalidade da auditoria de conformidade relativa à proteção de dados na Hungria consistia em avaliar se o quadro regulamentar e operacional da proteção de dados tinha sido instituído na Hungria e se as grandes organizações de gestão de dados tinham cumprido os requisitos relativos à gestão segura dos dados e à subcontratação do tratamento de dados. A auditoria incidiu, em especial, na proteção de dados pessoais e dos recursos de dados nacionais.

No contexto da auditoria, a ISC avaliou a gestão de dados realizada por seis organizações de gestão de dados (por exemplo, a autoridade tributária, o Tesouro nacional, os seguros de saúde, o pagamento de pensões, o departamento de educação, os dados e endereços pessoais, os registos de veículos e viagens, bem como os organismos administrativos para gestão dos dados criminais), além das atividades da autoridade de proteção de dados e da autoridade de segurança da informação.

A auditoria colocou especial ênfase no mandato das organizações de gestão de dados, em especial no caso de transferências de dados para terceiros. Durante a auditoria dos controlos internos relativos à gestão e ao tratamento dos dados, foram avaliados a existência de regulamentos atualizados sobre obrigações, responsabilidades e competências, a gestão dos recursos humanos e os processos.

A ISC avaliou as medidas de segurança relacionadas com os sistemas eletrónicos utilizados na gestão de dados, incluindo os seguintes domínios: proteção física, direitos de acesso, registo de dados, processos de avaliação da segurança, segurança do sistema e das comunicações e conformidade da classificação de segurança da organização no seu conjunto.

A subcontratação do tratamento de dados foi auditada com base nos contratos celebrados, tendo a ISC verificado se as organizações de gestão de dados obrigaram as organizações de tratamento de dados a cumprir os requisitos relacionados com as atividades de tratamento, em conformidade com a legislação.

Constatações e conclusões

Com base na auditoria, a ISC da Hungria concluiu que os regulamentos internos das organizações de gestão de dados no que respeita a essas atividades de gestão asseguraram a proteção dos recursos de dados nacionais enquanto ativos nacionais, em conformidade com as disposições jurídicas em vigor entre 2011 e 2015. Na prática, os responsáveis pelo tratamento dos dados tinham aplicado corretamente os requisitos em matéria de gestão segura dos dados e subcontratação do tratamento de dados. A transferência de dados para terceiros foi executada com um mandato adequado e uma definição clara das responsabilidades e poderes.

No caso de alguns responsáveis pelo tratamento dos dados, constatou-se que a classificação de segurança dos sistemas eletrónicos e da organização no seu conjunto nem sempre estava em conformidade com os requisitos jurídicos, sem que, no entanto, a dimensão destas deficiências tenha afetado substancialmente a segurança dos dados tratados. Com base nas recomendações incluídas no relatório de auditoria, as deficiências foram resolvidas pelas organizações de gestão de dados ao abrigo de planos de ação aprovados pela ISC.

No contexto da auditoria internacional realizada paralelamente em cooperação com o grupo de trabalho da EUROSAI sobre a informática, a ISC concluiu que a legislação húngara em matéria de proteção de dados estava em conformidade com a diretiva da UE em vigor.

Em conclusão, ao auditar a proteção de dados, a ISC da Hungria contribuiu para a boa governação e a proteção dos recursos de dados nacionais.

Outros relatórios no mesmo domínio

Título do relatório:	Relatório – Auditorias de seguimento – Auditoria relativa à proteção de dados – Auditoria do quadro nacional de proteção de dados e alguns registos de dados essenciais no âmbito da cooperação internacional
Hiperligação para o relatório:	Relatório (versão em língua húngara)
Data de publicação:	2020

Países Baixos
Tribunal de Contas

Cibersegurança das estruturas de importância crítica de gestão da água e de controlo das fronteiras nos Países Baixos

Datas de publicação: Março de 2019 e abril de 2020

Hiperligações para os relatórios: Resumo do relatório sobre a cibersegurança e as estruturas de importância crítica de gestão da água (versão em língua inglesa)

Resumo do relatório sobre a cibersegurança e os controlos automatizados nas fronteiras (versão em língua inglesa)

Tipo e período de auditoria

Tipo de auditoria: Auditoria de resultados

Período de auditoria: 2018-2020

Resumo do relatório

Tema da auditoria

Em 2018, o Tribunal de Contas dos Países Baixos decidiu realizar auditorias da cibersegurança em setores de importância crítica para a sociedade. Baseando-se na sua longa experiência de auditorias relativas à conformidade da segurança da informação na administração central, o Tribunal de Contas considerou que seria uma mais-valia auditar o *desempenho* das políticas e das medidas na prática. Os dois primeiros setores auditados foram a gestão da água e os controlos automatizados nas fronteiras: o primeiro é essencial para um país que se encontra maioritariamente abaixo do nível do mar e o segundo é importante devido à posição do aeroporto de Amesterdão-Schiphol como aeroporto central internacional e porta de entrada no país.

O Ministério das Infraestruturas e da Gestão da Água classificou várias estruturas hídricas geridas pela Direção-Geral das Obras Públicas e Gestão da Água (a entidade auditada) como "partes cruciais" do setor da gestão da água. Muitos dos sistemas

informáticos utilizados no funcionamento das estruturas de importância crítica de gestão da água remontam às décadas de 1980 e 1990, um período em que, normalmente, a cibersegurança não era tida em conta. Estes sistemas foram inicialmente concebidos para funcionamento autónomo, tendo sido gradualmente ligados a redes informáticas de maior dimensão, por exemplo, para facilitar o funcionamento à distância. Esta tendência tornou os sistemas mais vulneráveis a ciberameaças.

O Ministério da Defesa e o Ministério da Justiça e da Segurança são conjuntamente responsáveis pelos controlos nas fronteiras realizados pelos guardas de fronteira neerlandeses no aeroporto de Schiphol. Os guardas de fronteira utilizam sistemas informáticos dos dois ministérios (as entidades auditadas). Estes sistemas são essenciais para as operações nos aeroportos e são utilizados para tratar dados altamente sensíveis, constituindo, por isso, um alvo apetecível para ciberataques que visam a sabotagem, a espionagem ou a manipulação dos controlos nas fronteiras.

As auditorias examinaram a forma como as entidades auditadas estavam preparadas para responder a ciberameaças e se o faziam com eficácia.

- Questões de auditoria com vista a responder às seguintes perguntas: de que forma as entidades auditadas *protegem* os sistemas contra ciberameaças e *evitam* ciberataques?
- de que forma as entidades auditadas *detetam* ciberameaças e ciberataques?
- de que forma as entidades auditadas *respondem* a situações em que ocorre um ciberataque?

Um dos principais temas de ambas as auditorias foi a eficácia. Em estreita cooperação com as entidades auditadas, alguns *hackers* bem-intencionados exploraram estruturas de importância crítica de gestão da água e um dos sistemas de controlos nas fronteiras. Naturalmente, todas as constatações dos testes foram abordadas antes da publicação dos relatórios, sem que tenham sido divulgados pormenores técnicos.

A principal diferença entre as duas auditorias residiu no facto de a auditoria das estruturas de gestão da água se centrar no cumprimento das metas da entidade auditada, enquanto a auditoria dos controlos nas fronteiras se basear no enquadramento de cibersegurança do NIST.

Constatações

Em primeiro lugar, as duas auditorias constataram que as entidades auditadas tinham conhecimento das ciberameaças e estavam a aplicar uma abordagem profissional neste domínio.

Contudo, no caso das estruturas de gestão da água, a entidade auditada teria ainda de melhorar a sua deteção e resposta para cumprir as suas próprias metas de cibersegurança. A entidade auditada criou um Centro de Operações de Segurança (COS) para detetar e dar resposta aos ciberataques, mas o objetivo estabelecido para o final de 2017, ou seja, a deteção imediata de quaisquer ciberataques contra estruturas de importância crítica de gestão da água, não tinha sido alcançado até ao outono de 2018. Consequentemente, existia o risco de não detetar um ciberataque contra uma estrutura de importância crítica de gestão da água, ou de o detetar tardiamente. Além disso, o teste realizado numa dessas estruturas demonstrou que era possível aceder-lhe fisicamente. Os *hackers* conseguiram aceder à sala de controlo e ficaram sozinhos em estações de trabalho desprotegidas. Por último, a entidade auditada não elaborou um cenário de crise provocada por um ciberataque e não existiam ou não estavam atualizadas as informações relacionadas com a resposta a esta situação. A existência de informações atualizadas poderia revelar-se fundamental para uma resposta rápida e eficaz a uma situação de crise.

No que diz respeito aos controlos nas fronteiras, as medidas de cibersegurança não eram adequadas nem estavam preparadas para o futuro. Em primeiro lugar, os sistemas importantes de controlos nas fronteiras tinham de ser formalmente aprovados antes de começarem a funcionar, de modo a assegurar a aplicação de todas as medidas de cibersegurança. A auditoria constatou que dois dos três sistemas estavam a funcionar sem aprovação, pelo que não existiam garantias de que as medidas de segurança necessárias estivessem em vigor. Em segundo lugar, um COS estava a funcionar sem ligação direta a qualquer um dos sistemas. Embora existissem infraestruturas genéricas ligadas ao COS, continuava a existir o risco de os ciberataques não serem detetados ou de o serem tardiamente. Em terceiro lugar, não eram realizados regularmente testes de segurança. Com efeito, só um dos três sistemas tinha sido testado no passado, e apenas de forma limitada. Por último, tal como na primeira auditoria, não tinha sido elaborado um cenário específico para uma situação de crise provocada por um ciberataque.

Durante o teste de segurança de um dos sistemas que nunca tinha sido testado, os *hackers* bem-intencionados encontraram várias vulnerabilidades, que, em conjunto, podiam ser exploradas por um agente interno mal-intencionado e não autorizado para

lançar um ciberataque com vista a aceder, copiar e até manipular informações no sistema. Estes resultados demonstram a importância dos testes de segurança regulares.

As constatações são preocupantes devido à automatização em curso dos processos nas fronteiras. Num futuro próximo, um número crescente de sistemas de controlos nas fronteiras tratará cada vez mais dados utilizando um número cada vez maior de ligações. Uma vez que esta situação aumenta o risco de ciberataques, a abordagem utilizada não está preparada para o futuro.

Conclusões

No caso das estruturas de gestão da água, alguns elementos fundamentais impediram a entidade auditada de tomar as medidas de cibersegurança finais. Por exemplo, o nível da ameaça não era claro, o que torna difícil determinar se as medidas tomadas e o orçamento atribuído eram suficientes. Além disso, o departamento central responsável pela cibersegurança não possuía um mandato para aplicar as medidas de cibersegurança necessárias nas estruturas descentralizadas de gestão da água. As recomendações de auditoria foram seguidas a este respeito, contribuindo para a evolução da organização.

No caso dos controlos nas fronteiras, não existia uma justificação clara para o nível insuficiente de cibersegurança. O trabalho de investigação da auditoria detetou procedimentos e políticas de cibersegurança completos e pormenorizados, bem como conhecimentos especializados e trabalhadores qualificados suficientes. Por conseguinte, as recomendações da auditoria centraram-se essencialmente em assegurar que todas as medidas possíveis fossem, de facto, tomadas.

As duas auditorias suscitaram muito interesse do Parlamento e dos meios de comunicação social, aumentando a sensibilização para a cibersegurança em infraestruturas vitais e oferecendo às entidades auditadas indicações sobre formas de melhorar a sua cibersegurança. A cooperação estreita com a entidade auditada foi essencial para compreender plenamente a sua situação e abordar os riscos associados à investigação e aos testes da cibersegurança.

Está igualmente prevista uma terceira auditoria nesta série. Além disso, o nível de segurança da informação da administração central dos Países Baixos é um elemento fundamental do ciclo anual das auditorias de conformidade. Ao longo dos anos, a ISC dos Países Baixos constatou que muitos ministérios estão abaixo do esperado em termos de medidas de segurança da informação. O Tribunal de Contas utiliza

atualmente a experiência obtida nas suas auditorias da cibersegurança para alargar a sua perspetiva das auditorias da segurança da informação, indo além dos documentos e das políticas e testando a eficácia real das medidas.

Outros relatórios no mesmo domínio

Título do relatório:	Capítulo 3 do documento "*Staat van de rijksverantwoording 2019*"
Hiperligação para o relatório:	Relatório (versão em língua neerlandesa)
Data de publicação:	2020

Título do relatório:	Análise específica do teletrabalho digital
Hiperligação para o relatório:	Relatório (versão em língua neerlandesa)
Data de publicação:	2020

Polónia
Najwyższa Izba Kontroli

Garantir a segurança do funcionamento dos sistemas informáticos utilizados para executar tarefas públicas

Data de publicação: 2016

Hiperligação para o relatório: Relatório (versão em língua polaca)

Tipo e período de auditoria

Tipo de auditoria: Conformidade

Período auditado: 2014-2015

Resumo do relatório

Tema da auditoria

A auditoria tinha como objetivo avaliar, nas unidades auditadas, a segurança dos dados recolhidos nos sistemas destinados a executar tarefas públicas importantes. A auditoria abrangeu seis instituições selecionadas que executavam tarefas públicas significativas. Após uma análise, foi selecionado e examinado em pormenor um sistema informático essencial em cada uma das instituições. Foi aplicada na auditoria a versão 4.1 da metodologia COBIT (*Control Objectives for Information and related Technology*).

Esta auditoria foi realizada no seguimento da auditoria de 2015 sobre a execução das tarefas de cibersegurança pelos organismos públicos na Polónia[67], cujas constatações salientaram problemas sistémicos. A auditoria de 2016 demonstrou, nomeadamente que a administração pública não tinha tomado medidas, até então, para assegurar a segurança informática a nível nacional. Concluiu também que as atividades das entidades públicas relacionadas com a proteção do ciberespaço tinham sido executadas de forma fragmentada e sem uma abordagem sistémica. Na ausência de

[67] https://www.nik.gov.pl/kontrole/P/14/043/

mecanismos centrais para assegurar as condições de segurança concretas para sistemas informáticos específicos, essenciais para o funcionamento do Estado, a auditoria pretendia examinar se as instituições que administravam os sistemas informáticos utilizados para executar tarefas públicas importantes garantiam a segurança dessa execução.

Em 2019, foi aprovada uma outra auditoria de sistemas relacionada com a cibersegurança, intitulada "Cibersegurança na Polónia", mas as suas constatações são confidenciais.

Questões de auditoria

Os subobjetivos foram divididos em dois domínios de avaliação, procurando dar resposta a questões específicas.

No domínio do apoio à segurança informática, a nível da organização no seu conjunto a auditoria examinou, entre outros aspetos, se:

- a gestão da segurança informática era realizada;
- os planos para garantir a segurança informática eram executados;
- a segurança informática era testada, supervisionada e acompanhada;
- os incidentes de segurança informática estavam definidos;
- a gestão informática era realizada através de chaves criptográficas;
- a proteção contra *software* malicioso, a sua deteção e os *patches* eram aplicados;
- a segurança da rede era garantida.

No domínio do apoio à segurança, a nível dos sistemas selecionados a auditoria examinou, entre outros aspetos, se:

- a identidade e as contas dos utilizadores eram geridas;
- as tecnologias de segurança e os dados sensíveis estavam protegidos.

Constatações e conclusões

O grau de preparação e de aplicação do Sistema de Segurança da Informação não proporcionava um nível aceitável de segurança dos dados recolhidos nos sistemas informáticos destinados a executar tarefas públicas importantes. Os processos de segurança da informação eram executados de forma desordenada e, dada a ausência de procedimentos, intuitiva. Entre as seis unidades auditadas, apenas uma tinha aplicado o Sistema de Segurança da Informação, e deve notar-se que o funcionamento do sistema apresentava também falhas significativas. Em todas as unidades auditadas, com exceção de uma, o trabalho destinado a garantir condições de segurança adequadas às informações tratadas nos sistemas informáticos não tinha atingido o nível adequado, uma vez que, sendo um trabalho recente, se encontrava numa fase preliminar, que também incluía a elaboração das bases formais necessárias. Este trabalho baseava-se, até então, em mecanismos simplificados ou informais assentes em boas práticas ou na experiência do pessoal da informática.

Em conformidade com a metodologia COBIT 4.1, a maturidade dos processos de gestão da segurança das informações nas várias unidades variava entre 1 (inicial/pontual) e 3 (definida), numa escala de 0 a 5, em que 5 é o valor máximo.

A responsabilidade por garantir a segurança informática nas unidades auditadas cabia ao coordenador de segurança, mas este, na prática, não tinha competência para gerir o processo na sua totalidade. Além disso, as tarefas em questão eram muitas vezes realizadas apenas por uma pessoa. Embora tivessem sido nomeadas equipas especializadas ou celebrados acordos com contratantes externos, não tinha sido realizada a análise necessária para determinar se os serviços prestados davam resposta às necessidades de segurança de uma unidade. As unidades auditadas tinham uma compreensão fragmentada e limitada da necessidade de garantir a segurança informática. A segurança dos dados era entendida essencialmente como uma responsabilidade e um domínio de intervenção do departamento de informática e não de todas as unidades organizacionais com tarefas oficiais, o que comprometia significativamente o desenvolvimento de sistemas de gestão coerentes da segurança informática em toda a instituição.

Comparando a qualidade do cumprimento das obrigações destinadas a garantir a segurança da informação no âmbito das organizações, por um lado, e no âmbito dos sistemas selecionados, por outro, verifica-se que essa qualidade era superior no segundo caso. Esta situação poderá dever-se ao impacto do conhecimento prático e da participação do pessoal técnico de nível intermédio na garantia da segurança, à utilização acrescida, na administração pública, de sistemas informáticos comerciais

baseados nas normas do mercado e ao recurso a soluções avançadas de garantia da segurança. A aplicação destas soluções, da experiência adquirida e de boas práticas permitiu manter um certo nível de segurança no funcionamento dos vários sistemas num contexto de recursos limitados, insuficiências organizacionais ou regulação "não funcional". Contudo, esta não pode ser a solução visada, uma vez que, num período de aumento dinâmico do nível de ameaça, a segurança dos sistemas informáticos não pode basear-se em medidas geridas de forma desordenada e destinadas apenas a superar dificuldades imediatas.

Conclusões da auditoria

As recomendações e os requisitos gerais em matéria de segurança informática aplicáveis a todas as entidades públicas devem ser desenvolvidos e aplicados a nível central. É necessária uma solução sistémica, que divulgue os resultados das auditorias da segurança informática de forma a permitir o acesso dos cidadãos a informações sobre as atividades das entidades públicas, mas também limite o acesso ao conhecimento sobre as medidas e os métodos utilizados para garantir a segurança da informação tratada.

Outros relatórios no mesmo domínio

Título do relatório:	Gestão da segurança da informação pelas autoridades regionais
Hiperligação para o relatório:	Relatório (versão em língua polaca)
Data de publicação:	2019

Título do relatório:	A cibersegurança na Polónia (informações classificadas)
Hiperligação para o relatório:	*Não acessível ao público*
Data da aprovação:	2019

Título do relatório:	Garantia da segurança dos sistemas informáticos pelas autoridades regionais no voivodato da Podláquia
Hiperligação para o relatório:	Relatório (versão em língua polaca)
Data de publicação:	2018

Título do relatório:	Prevenção e combate da ciberintimidação entre crianças e jovens
Hiperligação para o relatório:	Relatório (versão em língua polaca)
Data de publicação:	2017

Título do relatório:	Desempenho das tarefas de cibersegurança pelos organismos públicos na Polónia
Hiperligação para o relatório:	Relatório (versão em língua polaca)
Data de publicação:	2015

Título do relatório:	Aplicação de requisitos específicos relativos aos sistemas de informação, ao intercâmbio eletrónico de informações e ao Quadro Nacional de Interoperabilidade com base no exemplo de algumas assembleias municipais e municípios com direitos distritais
Hiperligação para o relatório:	Relatório (versão em língua polaca)
Data de publicação:	2015

Portugal
Tribunal de Contas

Auditoria ao passaporte eletrónico português

Data de publicação: 2014

Hiperligação para o relatório: Relatório (versão em língua portuguesa)

Tipo e período de auditoria

Tipo de auditoria: Auditoria de resultados

Período de auditoria: 2013

Resumo do relatório

Tema da auditoria

A auditoria operacional ao passaporte eletrónico português (PEP) incidiu sobre a eficácia dos sistemas de informação que suportam a sua concessão, emissão e utilização, designadamente no controlo automatizado de passageiros através da leitura de dados biométricos nas fronteiras portuguesas[68].

A auditoria teve os seguintes objetivos principais:

- verificar o cumprimento do direito da UE e nacional, das normas internacionais e das orientações para a concessão, emissão e utilização do PEP, incluindo a adequação do quadro jurídico nacional;
- examinar a eficácia dos principais processos associados ao ciclo de vida do PEP, em especial os associados à concessão, emissão e utilização do PEP;

[68] Ver os sistemas automatizados de controlo nas fronteiras no âmbito da Frontex (Agência Europeia da Guarda de Fronteiras e Costeira).

- examinar os aspetos críticos do desempenho dos sistemas de informação, em especial a satisfação de requisitos de segurança relativos ao Sistema de Informação do Passaporte Eletrónico Português (SIPEP).

Os principais domínios de risco incluíam:

- o extravio/roubo de recursos físicos e/ou informações eletrónicas;
- a utilização inadequada de informações confidenciais;
- o risco de conformidade (não cumprimento dos requisitos jurídicos e regulamentares).

Período de auditoria: 1 de janeiro de 2013 – 31 de dezembro de 2013 (sempre que necessário, alargado a anos anteriores e posteriores).

Constatações e conclusões

O passaporte eletrónico português (PEP) abrange três categorias: comum[69], diplomático ou especial. Existe também um passaporte para estrangeiros, que confere menos privilégios.

O sistema de concessão contém vários requerimentos e diversas entidades de recolha de dados e entidades concedentes, mas apenas uma entidade emissora (incluindo produção, personalização e remessa).

Participam neste processo várias entidades (Entidades PEP). As seguintes entidades recolhem dados e concedem passaportes:

- em Portugal continental: o SEF[70] e os serviços de registo do IRN[71];

[69] Cerca de 99% do total.

[70] Serviço de Estrangeiros e Fronteiras.

[71] Instituto dos Registos e do Notariado (apenas receção).

- nas regiões autónomas dos Açores[72] e da Madeira: serviços integrados na respetiva VPGR[73]; no estrangeiro: os postos consulares portugueses;
- A INCM[74] procede à emissão e remessa dos passaportes.

Os principais processos são apoiados sobretudo pelo SIPEP (sistema de gestão centralizada dos requerimentos para a emissão dos passaportes portugueses). O SIPEP permite registar, armazenar, tratar, validar e disponibilizar a informação associada ao processo de concessão dos PEP, aciona o processo de personalização executado pela INCM e assegura a interligação com outros procedimentos de aquisição de dados do sistema, coordenando todas as entidades PEP que intervêm no registo físico e lógico dos dados recolhidos.

As Entidades PEP têm uma estrutura organizativa que lhes permite cumprir os objetivos legais associados ao PEP. O sistema ainda está fortemente dependente de recursos humanos aos níveis dos requerimentos e da recolha. Contudo, o SIPEP inclui várias funções de tratamento e controlos de validação automáticos.

Atendendo a que os procedimentos asseguram funções de controlo e manipulação de dados, que nalguns casos podem ser conduzidas de modo autónomo, sem intervenção humana, o SIPEP tem um significativo impacto quer ao nível da organização, quer do sistema de informação, designadamente, quanto: i) ao entendimento e definição das normas, processos e dados requeridos; ii) à definição dos requisitos do próprio sistema de informação.

A eficiência e a eficácia do processo de recolha de dados são asseguradas pela interação do SIPEP com outros sistemas de informação[75], em conformidade com os diplomas legais.

Foi estabelecido um quadro de controlo geral das atividades informáticas (governação, desenvolvimento e aquisição, operações informáticas, continuidade do serviço e recuperação de catástrofes, segurança da informação) que, embora não esteja

---

[72] E os pontos de serviço da Agência para a Modernização e Qualidade do Serviço ao Cidadão, I.P. (RIAC) (apenas receção).

[73] Vice-Presidência do Governo Regional.

[74] Imprensa Nacional – Casa da Moeda, empresa pública.

[75] Nomeadamente: Sistema Integrado de Informação do SEF (SIISEF); Parte Nacional do Sistema de Informação Schengen (NSIS); base de dados de identificação civil; base de dados do registo criminal.

amplamente documentado, assegura o desenvolvimento, o funcionamento, a gestão e a manutenção do SIPEP.

Indicadores de atividade (2013):

- foram concedidos cerca de 500 000 PEP, dos quais cerca de 63% pelo SEF, 33% pelos postos consulares e 4% pelos Governos Regionais;
- as receitas geradas pela emissão do PEP totalizaram cerca de 37 milhões de euros, destacando-se a INCM (43%), o SEF (32%) e o MNE[76] (17%).

Os testes efetuados no SIPEP não permitiram confirmar, para 2013, o cumprimento dos prazos máximos estabelecidos legalmente (desde a data do pedido da sua concessão até à disponibilidade do PEP para levantamento no ponto de entrega), uma vez que a data de entrega real no ponto de entrega nem sempre foi registada em tempo oportuno.

O SEF, o MNE, a RIAC e a INCM fizeram investimentos relacionados com a aquisição de equipamentos de recolha de assinatura e de dados biométricos (quiosques), de equipamentos para sistemas de controlo automatizado nas fronteiras e a aquisição e manutenção de sistemas informáticos, serviços e assistência técnica, num montante de 11 milhões de euros, a maior parte dos quais despendidos pelo SEF.

Antes do PEP, o preço do passaporte da República Portuguesa (não biométrico) era de 22,44 euros; o preço do PEP comum (biométrico) foi fixado em 60 euros em 2006 e em 65 euros em 2011.

Requerimentos do PEP

Os requerimentos do PEP são efetuados presencialmente nos serviços competentes, que procedem à receção dos documentos de instrução, à recolha dos dados biográficos e biométricos dos requerentes, à cobrança de taxas e, posteriormente à entrega do PEP emitido.

O sistema subjacente (SIPEP) valida a exatidão e a qualidade dos dados através de controlos virtuais e cruzamento com outros sistemas de informação, nomeadamente a base de dados de identificação civil, a fim de assegurar a conformidade e a adequação do requerimento para concessão e emissão do PEP.

[76] Ministério dos Negócios Estrangeiros.

As correspondentes mudanças de estados são conservadas em ficheiros de registo, o que assegura a possibilidade de controlo, a integridade e a não rejeição das operações.

A transmissão de dados entre os organismos de recolha de dados (em Portugal e no estrangeiro) e o SEF faz-se por linhas protegidas (VPN – *Virtual Private Network*), implementadas com base na gestão de acessos segundo credenciais geridas pelo SEF[77].

O pedido de PEP comum implica tratamento diferenciado nas situações em que seja apresentado por cidadãos cujo exercício de direitos esteja limitado ou condicionado, nomeadamente: i) incapazes (menores de idade, inabilitados ou interditos);
ii) impedidos judicial ou policialmente (registo criminal, pedidos de ação pendentes ou apreensão de documentos); iii) quando é alegado o interesse nacional ou legítimo do requerente para concessão de segundo PEP.

Concessão do PEP

A decisão de concessão do PEP comum pode ser:

- automatizada – deferimento automático do requerimento pelo SIPEP, após validações da identidade do requerente e da ausência de registo criminal (através do cruzamento com a base de dados de identificação civil do IRN e a base de dados do registo criminal) e de medidas cautelares. Só ocorre no SEF, relativamente a PEP requeridos no território continental[78];

[77] O SIPEP encontra-se acessível (via Web) a nível nacional/regional e internacional a serviços situados no continente, nas regiões autónomas dos Açores e da Madeira e no estrangeiro (postos consulares portugueses).

[78] Trata-se de uma funcionalidade do SIPEP de concessão automatizada (designada internamente por "deferimento") do requerimento (exceto de segundo PEP) de cidadão maior de idade, com cartão de cidadão válido, que não tenha medidas cautelares e não seja interdito ou inabilitado. Dos PEP comuns concedidos pelo SEF, cerca de 60% foram abrangidos pelos procedimentos de validação e decisão de concessão automatizada e os restantes foram objeto de análise e autorização na Direção Central de Imigração e Documentação (DCID).

- individualizada – sujeita a deferimento/autorização por outras entidades (Governos Regionais e postos consulares) ou, no caso do SEF, autorização dos requerimentos não abrangidos pela concessão automatizada[79].

Emissão do PEP

A emissão do PEP, abrangendo a produção, personalização e remessa, compete à INCM. O registo no SIPEP da entrega do PEP origina a alteração do estado deste para "Válido".

As taxas do PEP variam consoante o nível de serviço necessário. Para medir o nível de serviço, o SIPEP tem de considerar a data de entrega real do PEP.

A entrega do PEP é realizada por um serviço de transporte contratado.

Inutilização do PEP

Sempre que se verifique a entrega, pelo requerente, de PEP anterior válido, deve o mesmo ser inutilizado de modo a impedir a sua reutilização, o que corresponde à alteração do estado de registo do passaporte para "Inutilizado" no sistema de requerimentos do SIPEP.

[79] Nomeadamente, nos casos de requerentes incapazes (menores, interditos ou inabilitados), de impedimentos judiciais ou policiais e de segundo PEP, que são analisados caso a caso pela DCID.

Finlândia
Valtiontalouden tarkastusvirasto

Disposições de ciberproteção

Data de publicação: 2017

Hiperligação para o relatório: Relatório (versão em língua finlandesa)

Tipo e período de auditoria

Tipo de auditoria: Auditoria de resultados

Período de auditoria: 2016-2017

Resumo do relatório

Tema da auditoria

A auditoria tinha como objetivo verificar se a ciberproteção na administração central tinha sido configurada de forma tão eficaz e eficiente em termos de custos quanto possível. A auditoria incidiu sobre a forma de organização e gestão da cibersegurança da administração central. Os resultados da auditoria poderiam ser utilizados para reforçar a eficácia e a eficiência da cibersegurança na administração central. A auditoria decorreu entre 22 de setembro de 2016 e 4 de setembro de 2017. Na auditoria de seguimento, realizada no outono de 2019, a ISC examinou as medidas tomadas em resposta às constatações e recomendações da auditoria.

As entidades auditadas incluíram as autoridades responsáveis pela ciberproteção na administração central (o Gabinete do Primeiro-Ministro, o Ministério das Finanças e o Ministério dos Transportes e das Comunicações) e as autoridades responsáveis por tarefas centralizadas de ciberproteção e serviços informáticos centralizados na administração central (o Centro Nacional de Cibersegurança da Agência dos Transportes e das Comunicações da Finlândia, o Centro Nacional Valtori para as TIC e a Agência de Serviços de Dados Digitais e Populacionais). A avaliação da eficácia das orientações incluiu também um exame das unidades da administração central que prestam serviços eletrónicos (a Agência de Serviços de Dados Digitais e Populacionais,

a Agência dos Transportes e Comunicações da Finlândia, Traficom, o Gabinete Administrativo Nacional para Aplicação da Lei e a entidade que o supervisiona, o Ministério da Justiça, bem como o Centro de Serviços das TIC do Ministério da Justiça).

Questões de auditoria

A auditoria relativa à organização da cibersegurança utilizou as seguintes questões de auditoria:

- A entidade auditada teve suficientemente em consideração a vertente económica na organização da cibersegurança?
- O conhecimento situacional da entidade auditada em termos de cibersegurança contribuiu para a cibersegurança dos sistemas?
- A entidade auditada tem capacidade suficiente para responder a ciberviolações?

O tema de auditoria "Disposições de ciberproteção" inseria-se no tema geral de auditoria "Assegurar a fiabilidade operacional da sociedade da informação" constante do plano de auditoria da ISC finlandesa para 2016-2020. Do ponto de vista da importância para as finanças da administração central, o tema de auditoria justifica-se pelas desvantagens relacionadas com interrupções de serviço e violações de dados, bem como pelos efeitos negativos de uma cibersegurança insuficiente nas atividades institucionais. A auditoria decorreu paralelamente à auditoria intitulada "Orientação da fiabilidade operacional dos serviços eletrónicos", que se insere no mesmo tema geral. Os materiais de auditoria principais consistiam em documentos e entrevistas com as autoridades responsáveis pela atividade em questão.

Constatações e conclusões

A estratégia de cibersegurança da Finlândia define os principais objetivos e políticas utilizados para responder aos desafios enfrentados pelo ciberambiente e garantir o seu funcionamento. Foram desenvolvidos esforços para executar a estratégia de cibersegurança através de um programa de execução, cuja evolução é avaliada anualmente. O Comité de Segurança é um órgão de cooperação inserido no Ministério da Defesa que acompanha e coordena a execução da estratégia de cibersegurança.

Uma organização eficaz da cibersegurança implica a gestão dos riscos, a qual, para ter êxito, exige estruturas e mecanismos de gestão eficazes que integrem a gestão dos riscos nas operações em todos os níveis de uma organização. Como muitos outros

países, a Finlândia e a sua administração central não possuem recursos autónomos suficientes para garantir a ciberproteção. Ao longo do tempo, a legislação da União Europeia tornou-se mais numerosa e mais vinculativa. No Governo finlandês, a responsabilidade pela ciberproteção é descentralizada, sendo cada órgão institucional responsável pela sua própria cibersegurança. Na administração central, a atribuição de responsabilidades a respeito da natureza, da dimensão e da concretização de possíveis ciberviolações é complexa.

Devido a esta complexidade, a resposta a uma anomalia pode ser demasiado lenta, e a escassez de financiamento tem limitado a execução da estratégia de cibersegurança da Finlândia. Com base nas constatações da auditoria, a ISC formulou as conclusões e recomendações que se apresentam em seguida sobre a organização da cibersegurança na administração central.

A gestão operacional de violações graves da cibersegurança não foi definida

O planeamento relativo à gestão operacional de violações graves da cibersegurança e à repartição das responsabilidades correspondentes poderia permitir reações mais rápidas e uma coordenação e afetação de recursos adequadas para as contramedidas. No atual modelo operacional, cada organismo é responsável pela sua própria ciberproteção. Contudo, não está disponível conhecimento especializado suficiente em matéria de ciberproteção, o que impede que esta seja desenvolvida internamente ou através de subcontratação.

Alguns objetivos da estratégia de cibersegurança não foram alcançados

O programa de execução da estratégia de cibersegurança da Finlândia melhorou a ciberproteção. Alguns dos objetivos do primeiro programa de execução não foram alcançados, uma vez que o nível de compromisso com as ações variava e não podia ser melhorado de forma centralizada. O novo programa de execução apenas incluía ações que as autoridades competentes e outros intervenientes se tinham comprometido a executar. O nível de compromisso e os recursos disponíveis eram interdependentes.

Não era evidente que as soluções de financiamento da ciberproteção fossem adequadas

As diferenças no desenvolvimento da ciberproteção deviam-se, em parte, às diferenças no montante dos recursos de desenvolvimento que as organizações tinham ao seu dispor. Os regulamentos relativos à elaboração do orçamento do Estado ou ao respetivo processo não identificaram procedimentos para assegurar que os fundos eram afetados às metas mais importantes para a ciberproteção. Os organismos e as

instituições orçamentaram as dotações para a cibersegurança como uma parte não especificada das respetivas despesas operacionais. As medidas descritas na estratégia de cibersegurança da Finlândia foram aplicadas apenas na medida permitida pelas dotações.

As alterações na organização das TIC também devem ter em conta a ciberproteção

As alterações na organização das TIC na administração central influenciaram as disposições de ciberproteção. O desenvolvimento da cibersegurança centralizado pelo Valtori revelou-se difícil. Existiam deficiências na avaliação da adequação dos procedimentos práticos de ciberproteção e na aplicação de novas disposições.

O conhecimento situacional das operações de cibersegurança deve ser melhorado

O Centro de Cibersegurança mantinha um conhecimento situacional nacional da cibersegurança. À data da auditoria, não existia a obrigação de denunciar violações da cibersegurança ao Centro de Cibersegurança. A situação melhoraria se os organismos públicos fossem obrigados a denunciar as violações e se a cobertura dos procedimentos centralizados de deteção de ciberviolações aumentasse.

Com base nestas afirmações, a ISC recomenda que o Ministério das Finanças defina e aplique um modelo abrangente de gestão operacional para os casos de incidentes de cibersegurança nos serviços das TIC da administração central. O Ministério das Finanças deveria também procurar formas de ter em conta a cibersegurança no financiamento dos serviços ao longo do seu ciclo de vida e melhorar o conhecimento situacional operacional, incumbindo as autoridades de denunciar ciberviolações ao Centro de Cibersegurança. A ISC recomendou que o Valtori melhorasse a execução, a avaliação e o desenvolvimento dos procedimentos de cibersegurança e a deteção de ciberviolações.

A auditoria de seguimento examinou a execução das recomendações formuladas durante a auditoria inicial. A ISC considerou que o Ministério das Finanças, enquanto autoridade competente para a execução das recomendações, não tomou medidas suficientes em resposta às recomendações apresentadas. Contudo, a cibersegurança também tinha sido reforçada na Finlândia através de medidas tomadas por outras autoridades além do Ministério das Finanças. Estava em curso uma mudança na gestão estratégica da cibersegurança, no sentido de um modelo diretor da cibersegurança. Na proposta de orçamento para 2020, o Governo aumentou as dotações para as autoridades da administração central que desempenham um papel fundamental no reforço da cibersegurança. Além disso, o Valtori estava a tomar medidas em consonância com a recomendação da ISC. Em conclusão, a ISC afirmou que eram

necessárias auditorias de seguimento, devido à existência de recomendações que não foram executadas, e que se justificava uma auditoria de raiz neste domínio, devido às alterações em curso nas disposições de cibersegurança e no ambiente operacional digital, e aos riscos conexos, bem como à importância da cibersegurança para as finanças da administração central e para a sociedade.

Suécia
Riksrevisionen

Sistemas informáticos obsolescentes: um obstáculo a uma digitalização eficaz

Data de publicação: 2019

Hiperligação para o relatório: Resumo do relatório (versão em língua inglesa)
Relatório (versão em língua sueca)

Tipo e período de auditoria

Tipo de auditoria: Auditoria de resultados

Período de auditoria: 2018-2019

Resumo do relatório

Tema da auditoria

A obsolescência dos sistemas informáticos fundamentais para a atividade pode criar grandes problemas de eficiência, uma vez que, proporcionalmente, as organizações são obrigadas a mobilizar mais recursos apenas para manter o sistema. Por conseguinte, existem bons motivos para crer que os sistemas informáticos obsolescentes implicam um elevado risco de má gestão dos fundos públicos, bem como o desvio de uma parte da capacidade inovadora de um organismo em termos de desenvolvimento de novos sistemas informáticos. No entanto, além de criarem riscos para cada organismo isoladamente, os problemas criados pelos sistemas informáticos obsolescentes num organismo também podem ter consequências significativas na sua capacidade de coordenar operações com outro organismo ou com uma parte interessada privada. Os sistemas informáticos obsolescentes também implicam riscos do ponto de vista da segurança da informação.

Definição do principal tema da auditoria, das questões de auditoria e do contexto

A auditoria tinha como objetivo examinar a incidência de sistemas informáticos obsolescentes na administração central e avaliar se as autoridades e o Governo tinham tomado medidas adequadas para evitar que estes sistemas se tornassem um obstáculo a uma digitalização eficaz. Foram colocadas as seguintes questões de auditoria:

- As autoridades tomaram medidas adequadas para resolver os problemas associados a sistemas informáticos obsolescentes?
- O Governo tomou medidas adequadas para resolver os problemas associados a sistemas informáticos obsolescentes?

Constatações e conclusões

- A auditoria demonstrou que existiam sistemas informáticos obsolescentes num número elevado de organismos públicos. Além disso, em muitos organismos, um ou mais sistemas informáticos fundamentais para a atividade encontravam-se obsolescentes. Tanto quanto é do conhecimento da ISC sueca, esta informação é nova e ninguém tinha anteriormente consciência da dimensão do problema na administração central. Cerca de 80% dos organismos afirmaram ter tido dificuldade em manter o nível de segurança da informação em um ou mais dos seus sistemas fundamentais para a atividade. Mais de uma em cada dez autoridades responderam que esta dificuldade se aplicava à totalidade ou à maioria dos sistemas.
- Uma parte significativa dos organismos examinados não abordava corretamente o desenvolvimento e a administração do apoio informático. Estes organismos não utilizavam as ferramentas existentes de desenvolvimento operacional para determinar a melhor forma de utilizar o apoio informático para ajudar a alcançar os objetivos de operações fundamentais. Por conseguinte, uma parte significativa dos organismos auditados não possuía uma descrição global da ligação entre estratégias, processos operacionais e sistemas. Assim, tinham dificuldade em analisar e compreender o impacto das mudanças nos objetivos da organização, o que tornava mais difícil definir uma situação futura desejável.
- Mais de metade das autoridades afirmou que não existia um modelo aprovado para gerir os seus sistemas informáticos e tomar decisões sobre os mesmos desde a fase de desenvolvimento do sistema até à sua eliminação progressiva – a chamada gestão do ciclo de vida. Segundo a ISC sueca, este facto indicava que a

gestão do ciclo de vida não era estruturada nem metódica. Existiam também insuficiências no trabalho de análise dos riscos e na capacidade de repartir os custos informáticos com o nível de pormenor suficiente para uma tomada de decisões adequada.

- Quase 60% das autoridades não tinham planos de desenvolvimento para o ciclo de vida dos sistemas, com exceção de um ou alguns sistemas fundamentais para a atividade. A ausência, em muitos organismos, de planos para o ciclo de vida e outros documentos de planeamento, juntamente com as insuficiências na gestão do ciclo de vida efetivamente realizada, não permitiam considerar que os organismos em geral tivessem desenvolvido uma posição consciente e explícita relativamente aos seus sistemas informáticos.

- Segundo a avaliação da ISC sueca, os ministérios envolvidos e, por conseguinte, o Governo não tinham um conhecimento suficiente quer da incidência, quer das consequências dos sistemas informáticos obsolescentes.

Concluiu-se globalmente que, à data da auditoria, a maior parte dos organismos não conseguia na prática responder eficazmente aos problemas associados a sistemas informáticos obsolescentes. A ISC sueca considerou que este problema era de tal forma grave e generalizado que constituía um obstáculo à prossecução de uma digitalização eficiente da administração pública. A auditoria demonstrou também que o Governo não tinha conhecimento suficiente da existência e das consequências dos problemas dos sistemas informáticos obsolescentes. Além disso, o Governo não tinha tomado medidas para resolver de forma mais direta o problema dos sistemas informáticos obsolescentes. Por conseguinte, segundo a avaliação da ISC sueca, não se podia considerar que o Governo tivesse tomado medidas suficientes para assegurar a redução ou eliminação dos problemas.

Outros relatórios no mesmo domínio

Título do relatório:	Facilitar a criação de uma empresa – esforços do Governo para promover um processo digital (RiR 2019:14)
Hiperligação para o relatório:	Resumo do relatório (versão em língua inglesa) Relatório (versão em língua sueca)
Data de publicação:	2019

Título do relatório:	Digitalização da administração pública – Uma administração mais simples, mais transparente e eficaz (RiR 2016:14)
Hiperligação para o relatório:	Resumo do relatório (versão em língua inglesa) Relatório (versão em língua sueca)
Data de publicação:	2016

Título do relatório:	Trabalho em matéria de segurança da informação em nove organismos (RiR 2016:8)
Hiperligação para o relatório:	Resumo do relatório (versão em língua inglesa) Relatório (versão em língua sueca)
Data de publicação:	2016

Título do relatório:	Cibercriminalidade: as forças policiais e os procuradores podem ser mais eficientes (RiR 2015:21)
Hiperligação para o relatório:	Resumo do relatório (versão em língua inglesa) Relatório (versão em língua sueca)
Data de publicação:	2015

União Europeia
Tribunal de Contas Europeu

Documento informativo: Desafios à eficácia da política de cibersegurança

Data de publicação: 2018

Hiperligação para o relatório: Relatório (23 versões linguísticas)

Tipo e período de auditoria

Tipo de auditoria: Análise de políticas

Período de auditoria: Abril-setembro de 2018

Resumo do relatório

Tema da análise

O documento informativo em questão, que não constitui um relatório de auditoria, visava dar uma visão geral do complexo panorama da política da UE em matéria de cibersegurança e assinalar os principais desafios à sua execução eficaz. Abrange a segurança das redes e das informações, a cibercriminalidade, a ciberdefesa e a desinformação.

O Tribunal baseou a sua apreciação numa análise dos documentos oficiais, posições escritas e estudos de terceiros disponíveis ao público. O trabalho de campo foi realizado entre abril e setembro de 2018, sendo tidos em conta acontecimentos ocorridos até dezembro de 2018. O Tribunal complementou o trabalho com um inquérito às Instituições Superiores de Controlo dos Estados-Membros e com entrevistas às principais partes interessadas das instituições da UE e representantes do setor privado.

Não existe uma definição normalizada de "cibersegurança". No sentido lato, abrange todas as garantias e medidas tomadas para defender os sistemas informáticos e os utilizadores contra acessos não autorizados, ataques e danos, de forma a assegurar a confidencialidade, a integridade e a disponibilidade dos dados. A cibersegurança implica prevenir e detetar ciberincidentes, responder-lhes e recuperar dos mesmos.

Estes incidentes podem ser propositados ou não e vão desde, por exemplo, a divulgação acidental de informações até ataques a empresas e infraestruturas de importância crítica, passando pelo roubo de dados pessoais e até pela interferência nos processos democráticos.

A pedra angular da política da UE é a Estratégia para a Cibersegurança, de 2013, cuja finalidade é tornar o ambiente digital da UE o mais seguro do mundo, defendendo, ao mesmo tempo, os valores e liberdades fundamentais. Tem cinco prioridades estratégicas: i) aumentar a ciber-resiliência; ii) reduzir a cibercriminalidade; iii) desenvolver a política e as capacidades no domínio da ciberdefesa; iv) desenvolver recursos industriais e tecnológicos para a cibersegurança; v) estabelecer uma política internacional em matéria de ciberespaço alinhada com os valores fundamentais da UE.

Constatações

Era difícil apreender o impacto da falta de preparação para um ciberataque, pois não existiam dados fiáveis. O impacto económico da cibercriminalidade quintuplicou entre 2013 e 2017, atingindo tanto governos como empresas, de grande como de pequena dimensão. O crescimento previsto para os prémios de seguro de riscos cibernéticos, de 3 mil milhões de euros em 2018 para 8,9 mil milhões de euros em 2020, espelha esta tendência. Apesar de 80% das empresas da UE terem tido pelo menos um incidente de cibersegurança em 2016, a consciencialização sobre os riscos ainda é preocupantemente reduzida. Entre as empresas da UE, 69% não estão cientes da sua exposição a ciberameaças ou estão-no de forma limitada e 60% nunca fizeram uma estimativa das potenciais perdas financeiras. De acordo com um inquérito global, um terço das organizações preferiria pagar um resgate ao *hacker* do que investir na segurança da informação.

As conclusões do Tribunal foram as seguintes:

- o ecossistema cibernético da UE é complexo e multifacetado, envolvendo muitos intervenientes, e reunir todas as suas diferentes partes é um desafio considerável;

- a UE visa tornar-se o ambiente *online* mais seguro do mundo, uma ambição que exige esforços significativos de todas as partes interessadas e em particular uma base financeira sólida e bem gerida. É difícil obter números, estimando-se contudo que as despesas públicas da UE em matéria de cibersegurança se situem entre um e dois mil milhões de euros por ano. Comparativamente, as despesas públicas federais dos EUA ascenderam a cerca de 21 mil milhões de dólares orçamentados em 2019;

- a governação da segurança da informação implica instituir estruturas e políticas que garantam a confidencialidade, integridade e disponibilidade dos dados. Mais do que uma mera questão técnica, exige uma verdadeira liderança, processos sólidos e estratégias adaptadas aos objetivos da organização;

- os modelos de governação da cibersegurança variam consoante os Estados-Membros e, dentro de cada um, a responsabilidade nesta matéria está frequentemente repartida entre muitas entidades. Estas diferenças podem entravar a cooperação que é necessária para dar resposta a incidentes transfronteiriços em grande escala e para o intercâmbio de informações sobre ameaças a nível nacional e, ainda mais, a nível da UE;

- conceber uma resposta eficaz aos ciberataques é fundamental para os deter o mais cedo possível. É particularmente importante que os setores de importância crítica, os Estados-Membros e as instituições da UE sejam capazes de reagir de forma rápida e coordenada, sendo a deteção precoce essencial para esse fim.

Recomendações

A análise do Tribunal demonstra que é necessária uma transição para uma cultura de desempenho com práticas de avaliação integradas, de forma a garantir uma verdadeira prestação de contas e avaliação. Subsistem algumas lacunas legais, e os Estados-Membros não transpõem a legislação vigente da mesma forma, o que pode dificultar a concretização de todo o seu potencial.

Outro desafio apontado diz respeito à adaptação dos níveis de investimento aos objetivos estratégicos, o que requer um aumento dos níveis de investimento e do seu impacto e se torna mais exigente quando a UE e os Estados-Membros não dispõem de uma visão geral clara das despesas da UE no domínio da cibersegurança. Além disso, foram comunicadas restrições quanto à atribuição dos recursos adequados às agências da UE com responsabilidades na cibersegurança, designadamente dificuldades em atrair e reter talentos.

Siglas e acrónimos

AED: Agência Europeia de Defesa

APA: ameaça persistente avançada

CERS: Comité Europeu do Risco Sistémico

CERT-UE: equipa de resposta a emergências informáticas

COBIT: *Control Objectives for Information and Related Technology* (Objetivos de controlo para a tecnologia da informação e tecnologias conexas)

COVID-19: doença por coronavírus 2019

CSIRT: equipa de resposta a incidentes de segurança informática

DDoS: ataque distribuído de negação de serviço

Diretiva SRI: Diretiva Segurança das Redes e da Informação

EC3: Centro Europeu da Cibercriminalidade da Europol

ENISA: Agência da União Europeia para a Cibersegurança

EUA: Estados Unidos da América

Europol: Agência da União Europeia para a Cooperação Policial

FEEI: Fundos Europeus Estruturais e de Investimento

IdC: Internet das coisas

ISACA: *Information Systems Audit and Control Association* (Associação de auditoria e controlo dos sistemas de informação)

ISC: Instituições Superiores de Controlo

MERS: *Middle East Respiratory Syndrome* (síndrome respiratória do Médio Oriente)

MIE: Mecanismo Interligar a Europa

NATO: Organização do Tratado do Atlântico Norte

PCSD: Política Comum de Segurança e Defesa

PIB: Produto Interno Bruto

PPPc: parceria público-privada contratual

QFP: quadro financeiro plurianual

RGPD: Regulamento Geral sobre a Proteção de Dados

RH: recursos humanos

SARS: síndrome respiratória aguda grave

SEAE: Serviço Europeu para a Ação Externa

TCE: Tribunal de Contas Europeu

TIC: tecnologias da informação e comunicação

UE: União Europeia

URL: *Uniform Resource Locator* (Localizador uniforme de recursos)

Glossário

5G: norma tecnológica de quinta geração para redes móveis de banda larga, que as empresas de telemóveis começaram a implantar a nível mundial em 2019, como sucessora prevista das redes 4G, que asseguram a conectividade da maioria dos telemóveis atuais. O aumento da velocidade é conseguido, em parte, pela utilização de ondas de rádio com uma frequência mais elevada do que as redes móveis anteriores.

***Adware* (*software* de publicidade não solicitada):** *software* malicioso que apresenta faixas publicitárias ou janelas instantâneas (*pop-ups*) que incluem código destinado a rastrear o comportamento das vítimas na Internet.

Ameaça híbrida: manifestação de intenções hostis por parte de adversários através de uma combinação de técnicas de guerra convencionais e não convencionais (ou seja, métodos militares, políticos, económicos e tecnológicos) destinadas a atingirem pela força os seus objetivos.

Ameaças persistentes avançadas: ataques em que um utilizador não autorizado consegue aceder a um sistema ou rede e aí permanece durante um longo período de tempo sem ser detetado. São particularmente perigosas para as empresas, uma vez que os *hackers* têm acesso contínuo a dados empresariais sensíveis, embora, geralmente, sem provocar danos nas redes ou nos equipamentos locais das empresas. O objetivo destas ameaças é roubar dados.

Ataque distribuído de negação de serviço (DDoS): ciberataque que impede o acesso dos utilizadores legítimos a um serviço ou recurso em linha através do envio em massa de mais pedidos do que esse serviço ou recurso consegue tratar.

Ataques na Internet: ataques baseados na convicção dos utilizadores de que as informações pessoais sensíveis que divulgam num sítio Web serão mantidas privadas e seguras. Uma intrusão (ataque) pode tornar públicas as informações do cartão de crédito, da segurança social ou dos registos médicos do utilizador, com potenciais consequências graves.

Ativo digital: qualquer elemento existente em formato digital, detido por uma pessoa ou uma empresa, que está associado a um direito de utilização (por exemplo, imagens, fotografias, vídeos, ficheiros com texto, etc.).

***Bitcoin*:** uma moeda digital ou virtual criada em 2009 que utiliza tecnologia posto-a-posto para facilitar pagamentos imediatos.

Cavalo de Troia: tipo de código ou *software* malicioso que parece legítimo, mas pode assumir o controlo de um computador pessoal. Um cavalo de Troia é concebido para danificar, perturbar, roubar ou, em geral, provocar danos em dados ou numa rede.

Ciberameaça: ato malicioso que visa danificar ou roubar dados ou perturbar de um modo geral o mundo digital.

Ciberataque: tentativa de prejudicar ou destruir a confidencialidade, integridade e disponibilidade de dados ou de um sistema informático através do ciberespaço.

Cibercriminalidade: diferentes atividades criminosas que envolvem computadores e sistemas informáticos como instrumentos ou alvos principais, entre as quais se encontram crimes tradicionais (por exemplo, fraude, falsificação e roubo de identidade), crimes relacionados com conteúdos (por exemplo, distribuição em linha de pornografia infantil ou incitamento ao ódio racial) e crimes específicos dos computadores e sistemas de informação (por exemplo, ataques contra sistemas de informação, ataques de negação de serviço, *malware* ou *ransomware*).

Ciberdefesa: subdivisão da cibersegurança que visa defender o ciberespaço através de meios militares e outras formas adequadas a fim de alcançar objetivos estratégico-militares.

Ciberdiplomacia: utilização de recursos diplomáticos e exercício de funções diplomáticas para proteger os interesses nacionais no que respeita ao ciberespaço. É conduzida, na totalidade ou em parte, por diplomatas, reunidos em formatos bilaterais (como o diálogo EUA-China) ou em fóruns multilaterais (como as Nações Unidas). Indo além do âmbito tradicional da diplomacia, os diplomatas também interagem com diversos intervenientes não estatais, como líderes de empresas da Internet (por exemplo, Facebook ou Google), empresários das tecnologias ou organizações da sociedade civil. A diplomacia pode implicar também a capacitação de vozes oprimidas noutros países através da tecnologia.

Ciberespaço: ambiente global intangível em que se realiza a comunicação em linha entre pessoas, *software* e serviços através de redes informáticas e dispositivos tecnológicos.

Ciberespionagem: ato ou prática de obter segredos e informações sem a autorização ou o conhecimento do titular das informações a partir de pessoas, concorrentes, rivais, grupos, governos e inimigos para obter vantagens pessoais, económicas, políticas ou militares utilizando a Internet, redes ou computadores individuais.

Ciberincidente: evento que, direta ou indiretamente, provoca danos ou ameaça a resiliência e segurança de um sistema informático e dos dados por ele tratados, guardados ou transmitidos.

Ciber-resiliência: capacidade de prevenir ciberataques e ciberincidentes, de se preparar para eles, de lhes resistir e de recuperar deles.

Cibersegurança (ciberproteção): todas as garantias e medidas tomadas para defender os sistemas e dados informáticos de acessos não autorizados e de ataques e danos, de forma a assegurar a sua disponibilidade, confidencialidade e integridade.

Computação de alto desempenho: capacidade de tratar dados e realizar cálculos complexos a altas velocidades.

Computação em nuvem: disponibilização de recursos informáticos e a pedido – como armazenamento e capacidade de computação ou de partilha de dados – através da Internet, mediante o acolhimento em servidores distantes.

Confidencialidade: proteção das informações, dados ou recursos contra o acesso ou divulgação não autorizados.

Conteúdos digitais: quaisquer dados – tais como texto, som, imagens ou vídeo – guardados em formato digital.

Criptomoeda: ativo digital que é emitido e trocado através de técnicas de encriptação, sem intermédio de um banco central. É aceite como meio de pagamento entre os membros de uma comunidade virtual.

Dados biométricos (biometria): cálculos físicos (como impressões digitais e olhos) ou comportamentais relacionados com as características humanas. Esta autenticação é utilizada na informática como forma de identificação e de controlo do acesso.

Dados de acesso: informações sobre a atividade de início e fim de sessão de um utilizador ao aceder a um serviço, por exemplo a hora, a data e o endereço IP.

Dados pessoais: informações relativas a uma pessoa identificável.

Desinformação: informação comprovadamente falsa ou enganosa que é criada, apresentada e divulgada para obter vantagens económicas ou para enganar deliberadamente o público, e que pode causar um prejuízo público.

Digitalização: processo de conversão de informação num formato digital, em que a informação é organizada por *bits*, cujo resultado é a representação de um objeto, imagem, som, documento ou sinal gerando uma série de números que descreve um conjunto discreto de pontos ou amostras.

Disponibilidade: garantia de acesso e utilização das informações de forma oportuna e fiável.

Ecossistema cibernético: comunidade complexa de dispositivos, dados, redes, pessoas, processos e organizações que interagem entre si e o ambiente de processos e tecnologias que influencia e apoia essas interações.

Encriptação: transformação de informações legíveis em código ilegível para as proteger. Para ler as informações, o utilizador tem de ter acesso a uma chave ou senha secretas.

Engenharia social: no domínio da segurança da informação, manipulação psicológica para induzir as pessoas a realizarem uma ação ou divulgarem informações confidenciais.

***Hacker* bem-intencionado:** pessoa (especialista em segurança informática) que penetra numa rede informática para testar ou avaliar a sua segurança, sem intenção maliciosa ou dolo.

***Hacker*:** pessoa que utiliza competências informáticas, de ligação em rede ou outras para obter acesso não autorizado a dados, sistemas informáticos ou redes.

Infraestruturas de importância crítica: recursos, serviços e instalações físicos cuja perturbação ou destruição teria um impacto grave no funcionamento da economia e da sociedade.

Infraestruturas eleitorais: incluem sistemas informáticos e bases de dados das campanhas eleitorais, informações sensíveis sobre os candidatos, o recenseamento dos eleitores e sistemas de gestão.

Instalações de serviços públicos: qualquer poste, torre, caminho aéreo ou subterrâneo, qualquer outra estrutura de apoio ou sustentação, e qualquer vala, com os respetivos acessórios, passível de ser utilizado para o fornecimento ou a distribuição de serviços elétricos, telefónicos ou telegráficos, de transporte de cabos ou de sinalização ou outro serviço similar.

Integridade: proteção contra a alteração ou destruição das informações de forma imprópria e garantia da sua autenticidade.

Inteligência artificial: simulação da inteligência humana em máquinas programadas para pensar como os seres humanos e imitar as suas ações; qualquer máquina que apresenta atributos associados à mente humana, como a aprendizagem e a resolução de problemas.

Internet das coisas (IdC): rede de objetos de uso quotidiano equipados com eletrónica, *software* e sensores que lhes permitem comunicar e trocar dados através da Internet.

***Malware*:** *software* malicioso. Programa informático destinado a provocar danos num computador, servidor ou rede.

Operador de serviços essenciais: entidade pública ou privada que presta um serviço essencial para a manutenção de atividades societais e económicas cruciais.

***Patching* (remendo):** introdução de um conjunto de alterações num *software* para o atualizar, reparar ou melhorar, incluindo corrigir vulnerabilidades em termos de segurança.

***Phishing*:** prática de enviar mensagens eletrónicas que aparentemente provêm de uma fonte fidedigna para enganar os destinatários e levá-los a clicar em ligações maliciosas ou a partilhar informações pessoais.

Plataforma digital: ambiente para interações entre pelo menos dois grupos diferentes, em que, geralmente, um é composto por fornecedores e o outro por consumidores/utilizadores. Pode tratar-se do *hardware* ou do sistema operativo, ou mesmo de um programa de navegação e das correspondentes interfaces de programação de aplicações, ou outro *software* subjacente, desde que seja utilizado para executar o código do programa.

Prestador de serviços digitais: qualquer entidade que presta um ou mais destes três tipos de serviço digital: mercado em linha, motores de busca e serviços de computação em nuvem.

Protocolo de ambiente de trabalho remoto: norma técnica (publicada pela Microsoft) para utilização de um computador pessoal à distância. Os utilizadores do ambiente de trabalho remoto podem aceder ao seu ambiente de trabalho, abrir e editar ficheiros e utilizar aplicações como se estivessem diante do seu computador pessoal.

***Ransomware* (*software* de sequestro):** *software* malicioso que impede que as vítimas acedam a um sistema informático ou torna os ficheiros ilegíveis, geralmente através de encriptação. Em geral, o autor do ataque faz então chantagem com a vítima, recusando-se a repor o acesso até que seja pago um resgate.

Sabotagem: ação destinada a destruir, danificar ou obstruir de forma deliberada, principalmente para obter vantagens políticas ou militares.

Segurança da informação: conjunto de processos e ferramentas que protegem dados físicos e digitais contra o acesso, utilização, divulgação, perturbação, alteração, registo ou destruição não autorizados.

Segurança das redes: subdivisão da cibersegurança que protege os dados enviados através de dispositivos da mesma rede com o fim de garantir que as informações não sejam intercetadas ou alteradas.

Sistema de informação de importância crítica: qualquer sistema de informação, existente ou previsto, considerado essencial para o funcionamento eficiente e eficaz da organização.

***Spyware* (*software* espião):** *software* com comportamento malicioso que visa recolher informações sobre uma pessoa ou organização e enviar essas informações a outra entidade de forma a lesar o utilizador, por exemplo violando a sua privacidade ou colocando em risco a segurança do dispositivo.

Tratamento de dados: realização de operações com dados, nomeadamente por um computador, para extrair, transformar ou classificar informações.

Vetorização de texto: processo de conversão de palavras, frases ou documentos completos em vetores numéricos para que possam ser utilizados por algoritmos de aprendizagem automática.

Violação de dados: divulgação, propositada ou não, de informações seguras ou privadas/confidenciais num ambiente não fidedigno.

***Worm* (verme):** programa informático autónomo de *malware* que se replica a fim de se propagar a outros computadores. Utiliza frequentemente uma rede informática para se propagar, tirando partido de falhas de segurança no computador-alvo para aceder ao mesmo.

Contactar a EU

Pessoalmente
Em toda a União Europeia há centenas de centros de informação Europe Direct. Pode encontrar o endereço do centro mais próximo em: https://europa.eu/european-union/contact_pt

Telefone ou correio eletrónico
Europe Direct é um serviço que responde a perguntas sobre a União Europeia. Pode contactar este serviço:
— pelo telefone gratuito: 00 800 6 7 8 9 10 11 (alguns operadores podem cobrar estas chamadas),
— pelo telefone fixo: +32 22999696, ou
— por correio eletrónico, na página: https://europa.eu/european-union/contact_pt

Encontrar informações sobre a UE

Em linha
Estão disponíveis informações sobre a União Europeia em todas as línguas oficiais no sítio Europa: https://europa.eu/european-union/index_pt

Publicações da UE
As publicações da UE, quer gratuitas quer pagas, podem ser descarregadas ou encomendadas no seguinte endereço: https://publications.europa.eu/pt/publications. Pode obter exemplares múltiplos de publicações gratuitas contactando o serviço Europe Direct ou um centro de informação local (ver https://europa.eu/european-union/contact_pt).

Legislação da UE e documentos conexos
Para ter acesso à informação jurídica da UE, incluindo toda a legislação da UE desde 1952 em todas as versões linguísticas oficiais, visite o sítio EUR-Lex em: https://eur-lex.europa.eu

Dados abertos da UE
O Portal de Dados Abertos da União Europeia (http://data.europa.eu/euodp/pt) disponibiliza o acesso a conjuntos de dados da UE. Os dados podem ser utilizados e reutilizados gratuitamente para fins comerciais e não comerciais.

Contact Committee

Comité de Contacto

das Instituições Superiores de Controlo da União Europeia