GESEL

Grupo de Estudos do Setor Elétrico

UFRJ

A segurança cibernética no setor elétrico da União Europeia: Uma análise da trajetória da regulação e das estratégias de superação de fragilidades

Vitor Santos
Lorrane Câmara
Mauricio Moszkowicz
Nivalde de Castro

TDSE

Texto de Discussão do Setor Elétrico

Nº 99

março de 2021
Rio de Janeiro

GESEL
Grupo de Estudos do Setor Elétrico
UFRJ

TDSE

Texto de Discussão do Setor Elétrico Nº 99

A segurança cibernética no setor elétrico da União Europeia: Uma análise da trajetória da regulação e das estratégias de superação de fragilidades

Vitor Santos
Lorrane Câmara
Mauricio Moszkowicz
Nivalde de Castro

ISBN: 978-65-86614-23-7

Março de 2021

Sumário

INTRODUÇÃO

As tendências recentes de desenvolvimento do setor elétrico, muito marcadas pela transição energética e pela descarbonização da economia, indicam que a segurança cibernética será uma dimensão crítica, com importância crescente nas próximas décadas.

O desenvolvimento das redes e da medição inteligente, a relevância da geração distribuída, o crescimento da mobilidade elétrica na prestação de serviços ao sistema e a valorização da gestão flexível da demanda contribuirão para a digitalização e automação crescentes do setor elétrico, que tenderão a se acentuar com a emergência das comunicações 5G. Soma-se a essa tendência o surgimento de novos agentes no setor elétrico, como os agregadores, os prestadores de serviços de flexibilidade e os prossumidores, contribuindo para um aumento expressivo no número de participantes no mercado e ampliando significativamente a vulnerabilidade do setor a ataques cibernéticos.

Segundo a classificação da Comunidade Europeia, o setor energético apresenta o maior grau de criticidade dentre todos os setores da economia, a exemplo dos setores financeiro e de saúde, também caracterizados pela prestação de serviços essenciais e pela presença de infraestruturas críticas. O racional adotado é que as instalações de energia são básicas para o funcionamento dos demais segmentos. Esta característica aprofunda os riscos e potenciais impactos de ataques cibernéticos ao setor elétrico.

A evidência empírica sugere que os ataques cibernéticos são cada vez mais frequentes e causam danos crescentemente mais expressivos (sobre este assunto, ver o Anexo I). Face a este contexto, a União Europeia definiu uma série de ações para estabelecer um arcabouço regulatório que promovesse a segurança cibernética no setor elétrico.

O presente documento tem por objetivo analisar a evolução e o processo de construção desse arcabouço. A estratégia implementada pela União Europeia

definiu fases, visando a aprovação da legislação adequada aos novos desafios suscitados pela segurança cibernética, destacando:

- Na primeira fase, as instâncias comunitárias procederam a aprovação, em 2016, da Diretiva sobre Segurança das Redes e da Informação (SRI) e do Regulamento Geral sobre a Proteção de Dados (RGPD), que permitem estabelecer as bases, transversais a todos os setores, para garantir a segurança cibernética no fornecimento dos serviços energéticos, bem como a proteção de dados no setor elétrico (vide Seção 1.1);
- Na segunda fase, como a Diretiva SRI sobre a segurança cibernética e o Regulamento GDPR sobre a proteção de dados apenas constituíram normas transversais, foi necessário estabelecer regras específicas para os diversos setores, incluindo o setor elétrico. Neste sentido, a Direção Geral da Energia da Comissão Europeia criou um grupo de especialistas, o *Energy Expert Cyber Security Platform* (EECSP), ao qual atribuiu a incumbência de identificar os *gaps* que existiam na legislação do setor energético, de modo a assegurar uma efetiva segurança cibernética (vide Seção 1.2); e
- Na terceira fase, na sequência do Acordo de Paris, a União Europeia aprovou, em 2019, um pacote legislativo com cinco dimensões para a União da Energia. Neste contexto, foram aprovados quatro documentos com grande relevância para a segurança cibernética no âmbito do setor elétrico (Seção 1.3).

Após a apresentação da legislação europeia sobre segurança cibernética, o trabalho procede a avaliação do seu impacto nos diferentes Estados-Membros, com base no relatório "*Cybersecurity Benchmark*", publicado em 2019, pelo Conselho Europeu dos Reguladores de Energia (CEER). Este relatório apresenta um estudo de *benchmarking* detalhado de 16 países membros da União Europeia, cujos principais resultados são apresentados na Seção 2.

Face à nova legislação europeia sobre a segurança cibernética e a proteção de dados, a Seção 3 procura identificar os novos desafios para os reguladores

setoriais europeus ao nível dos marcos regulatórios, na transformação das atitudes e da cultura organizacional dos operadores de bens essenciais e no compartilhamento e na disseminação das boas práticas.

Na Seção 4 é apresentado um panorama da segurança cibernética em Portugal, destacando três aspectos: o quadro nacional de referência para a segurança cibernética em uma perspectiva transversal, o enquadramento legislativo e regulatório no caso específico do setor elétrico e o papel da Entidade Reguladora dos Serviços Energéticos (ERSE) na promoção da segurança cibernética no país.

Na Seção 5, são analisadas as fragilidades na oferta de qualificações por parte dos sistemas de ensino, formação e Pesquisa e Desenvolvimento (P&D) em segurança cibernética nos países europeus. Face ao avanço do quadro regulatório europeu para a segurança cibernética, foram identificados *gaps* nas áreas de P&D e formação de mão-de-obra em segurança cibernética, o que motivou a definição de uma agenda integrando iniciativas que visavam superar as referidas fragilidades.

Esta agenda está definida no "*European Cybersecurity Strategic Research and Innovation Agenda for a Contractual Public-Private Partnership*", que aposta no envolvimento da indústria em parcerias público-privadas para promover projetos, com base nos princípios da neutralidade setorial e tecnológica e na maximização do potencial de replicação das tecnologias e das soluções. Neste sentido, a Seção 5 conta com a seguinte estrutura:

- Na Seção 5.1, são analisados os modelos de governança adotados nas instituições que foram utilizadas pela União Europeia como instrumento para o desenvolvimento do ensino, formação e inovação em segurança cibernética;
- Na Seção 5.2, são analisados quatro projetos piloto — CONCORDIA, ECHO, SPARTA e CyberSec4Europe —, que visam estabelecer centros de excelência com o objetivo inicial de definir um *roadmap* para a consolidação de um sistema comum europeu de pesquisa e inovação em segurança cibernética;

- Na Seção 5.3, é apresentado o EU CAIH, um centro de excelência da União Europeia para educação e treino em segurança cibernética e ciberdefesa, coordenado por Portugal e sediado em Lisboa, que se inspira, simultaneamente, no conceito de DIH e nos centros de excelência; e
- Na Seção 5.4, é apresentado um projeto de centro de excelência que poderá ser implementado no Brasil, trazendo a estrutura adotada na Comunidade Europeia para o setor elétrico nacional.

Finalmente, são discorridas as conclusões do trabalho, rebatendo os dados apresentados para uma análise sobre a possibilidade de implementá-los no setor elétrico nacional.

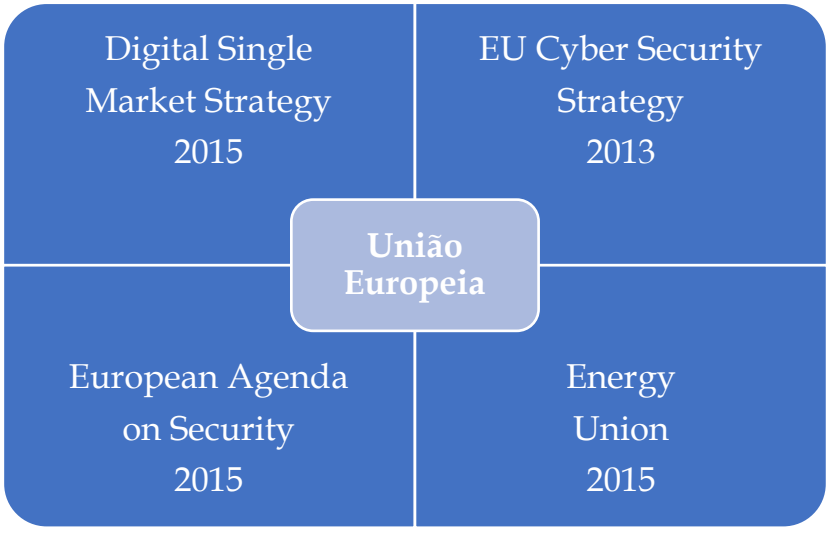
1 O ENQUADRAMENTO LEGISLATIVO: UNIÃO EUROPEIA

A legislação atual sobre segurança cibernética e proteção de dados conta com diferentes iniciativas promovidas pela União Europeia, conforme apresentado na Figura 1, destacando:

- A estratégia para o Mercado Único Digital na Europa;
- A estratégia para a Segurança cibernética na União Europeia;
- A agenda para a Segurança Europeia; e
- A União da Energia.

Estas iniciativas foram motivadas por uma preocupação comum com a segurança cibernética e a proteção dos dados.

Figura 1 - Antecedentes recentes da legislação da União Europeia sobre segurança cibernética e proteção de dados



Fonte: Elaboração própria.

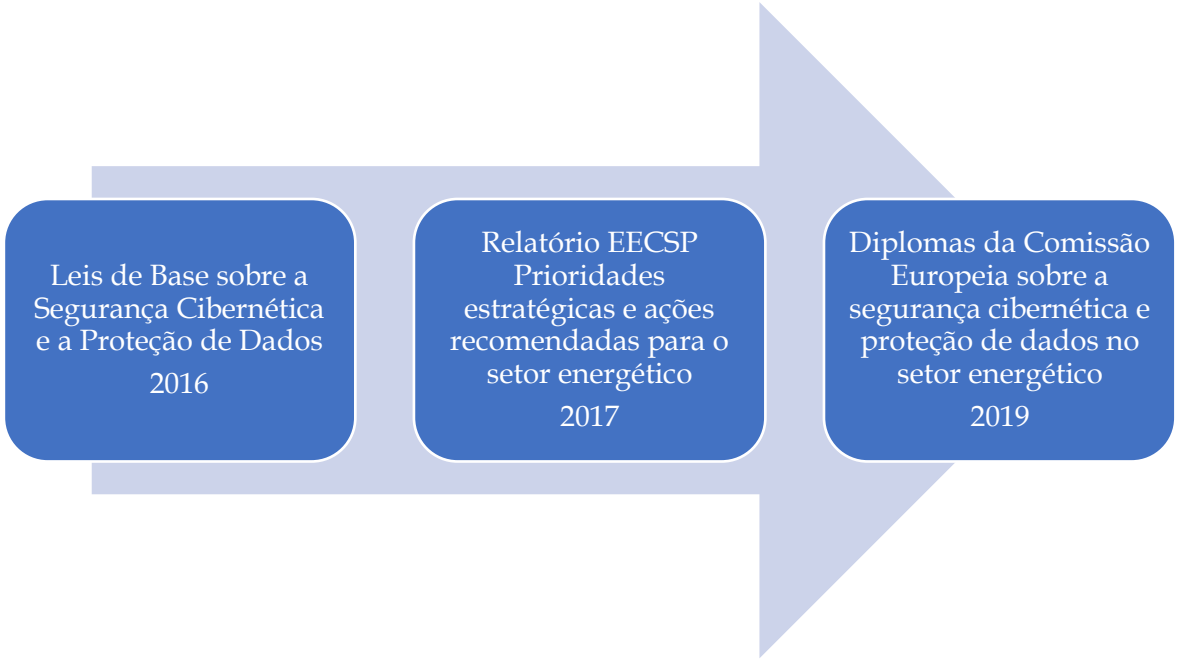
A legislação de base para a segurança cibernética e para a proteção de dados tem uma abordagem com a seguinte cronologia temporal (Figura 2 e Quadro 1), na qual se distinguem três etapas:

- A Diretiva Segurança das Redes e da Informação – SRI (*Directive on Security of Network and Information Systems* – NIS) e o Regulamento Geral sobre a Proteção de Dados – RGPD (*General Data Protection Regulation* –

GDPR), aprovados em 2016, estabelecem as bases para garantir a segurança cibernética e a proteção de dados em todos os setores de atividade que prestam serviços essenciais;

- O setor energético tem especificidades no âmbito da segurança cibernética e da proteção de dados que exigem uma análise técnica aprofundada destes temas. Com esta motivação, foi criado um grupo de trabalho de especialistas, o EECSP, que elencou as prioridades estratégicas e propôs, em 2017, recomendações em relação às ações a serem desenvolvidas neste setor; e
- A União Europeia publicou uma legislação, em 2019, visando a definição de normas relativas à segurança cibernética e à proteção de dados aplicáveis ao setor de energia, em geral, e ao setor elétrico, em particular. A maioria destas normas consta do Pacote "*Clean Energy for all Europeans*", aprovado em 2019.

Figura 2 - As três etapas da legislação



Fonte: Elaboração própria.

Quadro 1 - Enquadramento Jurídico

Diretiva Segurança das Redes e da Informação – SRI ***Network and Information Systems* (NIS) *Directive* (EU) 2016/1148** Estabelece as regras e o modelo de funcionamento do sistema de segurança cibernética europeu. Os Estados-Membros devem aprovar uma estratégia nacional de segurança cibernética, designar às autoridades nacionais competentes os pontos de contato únicos e as CSIRT (*Computer Security Incident Response Team*), com atribuições relacionadas à segurança das redes e dos sistemas de informação. Esta diretiva obriga os Operadores de Serviços Essenciais (em inglês, OES) a promoverem as medidas necessárias, de forma a reduzirem o risco de ataques cibernéticos, e a notificarem os governos nacionais sobre a sua ocorrência. As autoridades competentes nacionais monitorizam a aplicação da diretiva e participam no Grupo de cooperação da NIS que inclui, ainda, representantes da Comissão Europeia e da *European Union Agency for Network and Information Security* (ENISA). Em 2018, este Grupo criou uma área de trabalho dedicada à energia.
***Cybersecurity Act – Regulation* (EU) 2019/881** Este regulamento atribui à ENISA a responsabilidade pela coordenação e cooperação na segurança cibernética entre os Estados-Membros e as Instituições da União Europeia. Estabelece, ainda, o enquadramento ao sistema de certificações para as TIC, processos e serviços.
Regulamento Geral sobre a Proteção de Dados (RGPD) ***General Data Protection* – Regulation (EU) 2016/679** Este regulamento atualiza a 1995 *Data Protection Directive*, reforça os direitos individuais e o mercado interno da União Europeia, simplifica as transferências internacionais de dados e estabelece padrões globais para a proteção de dados.

1.1 Legislação sobre segurança cibernética e proteção de dados na União Europeia

A aprovação pelas instâncias comunitárias, em 2016, da Diretiva SRI e do RGPD permite estabelecer as bases, transversais a todos os setores, para garantir a segurança cibernética no fornecimento dos serviços energéticos, bem como a proteção de dados no setor elétrico. Os conteúdos básicos destes regulamentos são apresentados no Quadro 1, acima.

O preâmbulo da Diretiva SRI destaca que as capacidades existentes são insuficientes para garantir um nível adequado de segurança das redes e dos sistemas de informação na União Europeia. Os Estados-Membros registram níveis muito distintos de preparação, assim como uma elevada assimetria nas metodologias que são adotados pelos diferentes países. Esta situação traduz-se não só em um nível desigual de defesa dos consumidores e das empresas, mas também compromete o nível global de segurança das redes e dos sistemas de informação na União. Adicionalmente, a inexistência de requisitos mínimos comuns a serem adotados pelos operadores de serviços essenciais e pelos prestadores de serviços digitais impossibilita a criação de um mecanismo global e eficaz para a cooperação a nível europeu.

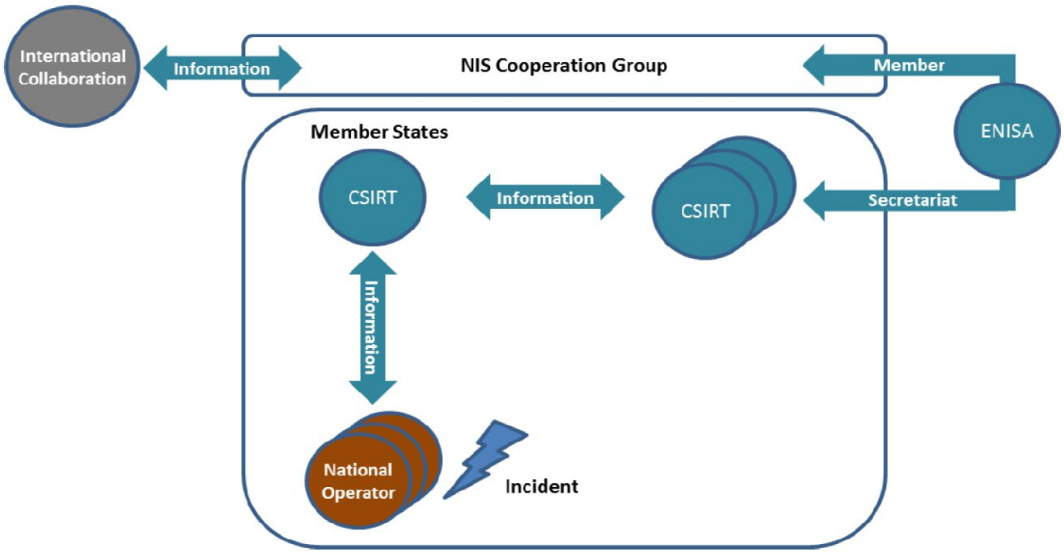
Neste contexto, a Diretiva SRI tem os seguintes objetivos:

a. Estabelecer a obrigação de os Estados-Membros adotarem uma estratégia nacional de segurança das redes e dos sistemas de informação;
b. Criar um grupo de cooperação a fim de apoiar e facilitar a colaboração estratégica e o intercâmbio de informações entre os Estados-Membros e de desenvolver a confiança entre eles. O grupo de cooperação é constituído por representantes dos Estados-Membros, da Comissão Europeia e da ENISA, que assegura o secretariado, conforme apresentado na Figura 3;
c. Criar uma rede de Equipes de Resposta a Incidentes de Segurança (rede de CSIRT) para promover uma cooperação operacional célere e eficaz;

d. Estabelecer requisitos de segurança e de notificação para os operadores de serviços essenciais e para os prestadores de serviços digitais; e

e. Estabelecer a obrigação de os Estados-Membros designarem às autoridades nacionais competentes os pontos de contato únicos e as CSIRT com atribuições relacionadas à segurança das redes e aos sistemas de informação.

Figura 3 - Grupo de Cooperação da Diretiva SRI



Fonte: EECSP (2017).

Conforme observado na Figura 3, a ENISA assegura os serviços de secretariado e apoia ativamente a cooperação entre as CSIRT, destacando as seguintes atribuições:

- Assistir os Estados-Membros e a Comissão Europeia, através da disponibilização de competências especializadas, bem como do aconselhamento e da facilitação do intercâmbio de boas práticas;
- Responder consultas da Comissão Europeia e dos Estados-Membros;
- Promover o intercâmbio de boas práticas e a discussão das capacidades para a preparação dos Estados-Membros; e
- Assistir os seus membros na avaliação das estratégias nacionais de segurança das redes e dos sistemas de informação, no reforço das suas

capacidades e na avaliação de exercícios de segurança das redes e dos sistemas de informação.

Uma resposta eficaz aos desafios que se colocam à segurança das redes e dos sistemas de informação exige, assim, uma abordagem global a nível da União Europeia em relação aos seguintes aspetos:

- Os requisitos mínimos comuns de desenvolvimento de capacidades e de planejamento;
- O intercâmbio de informações; e
- A cooperação e os requisitos comuns de segurança para os operadores de serviços essenciais e para os prestadores de serviços digitais.

Destaca-se que os operadores de serviços essenciais e os prestadores de serviços digitais não estão impedidos de aplicar medidas de segurança mais rigorosas do que as previstas na presente diretiva.

Para esse efeito, a Diretiva SRI prevê:

- A avaliação das entidades ativas em setores e subsetores específicos;
- A elaboração de uma lista de serviços essenciais;
- A análise de uma lista comum dos fatores entre setores para determinar se um potencial incidente teria um efeito perturbador importante;
- Um processo de consulta que envolva os Estados-Membros no caso de haver entidades que prestem serviços em mais de um deles;
- O apoio do grupo de cooperação no processo de identificação;
- A revisão regular da lista dos operadores identificados; e
- Que os Estados-Membros deverão prestar as informações necessárias à Comissão Europeia para que esta possa avaliar em que medida a metodologia comum permitiu aplicar coerentemente a definição.

Os Estados-Membros deverão dispor de CSIRT que preencham os requisitos essenciais para garantir capacidades efetivas e compatíveis para responder aos incidentes e aos riscos e para assegurar uma cooperação eficaz a nível da União

Europeia. Uma vez que a maioria das redes e dos sistemas de informação são explorados pelo setor privado, a sua cooperação com o setor público é essencial.

As medidas técnicas e organizacionais aplicáveis aos operadores de serviços essenciais e aos prestadores de serviços digitais deverão respeitar os seguintes critérios:

- O princípio da neutralidade tecnológica, isto é, não deverá ser exigido que um determinado produto das tecnologias da informação e da comunicação que tenha fins comerciais seja concebido, desenvolvido ou fabricado de um modo específico; e
- As medidas devem ser custo-efetivas, ou seja, os requisitos estabelecidos deverão balancear os riscos apresentados pelas redes e pelos sistemas de informação, considerando os progressos técnicos mais recentes.

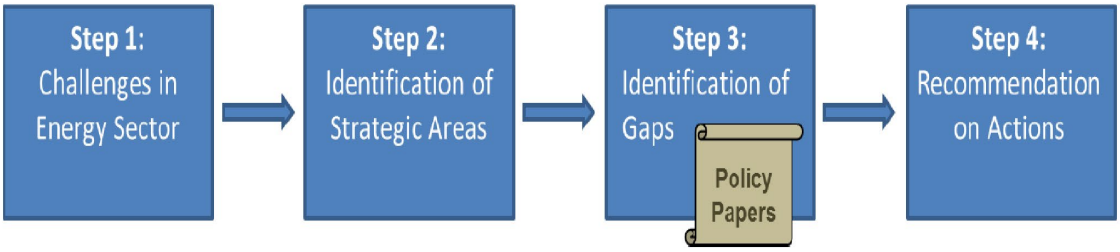
1.2 Legislação sobre segurança cibernética e proteção de dados na União Europeia e as especificidades do setor elétrico

A Diretiva SRI sobre a segurança cibernética e o Regulamento GDPR sobre a proteção de dados estabelecem normas transversais e, por isso, foi necessário estabelecer regras específicas para os diversos setores, incluindo o setor elétrico.

Neste sentido, a Direção Geral da Energia da Comissão Europeia criou um grupo de especialistas, o *Energy Expert Cyber Security Platform*, com a responsabilidade de identificar as lacunas que existiam na legislação do setor energético, de modo a assegurar uma efetiva segurança cibernética.

Em 2017, o EECSP publicou o relatório "*Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector*". A metodologia de análise estabeleceu quatro passos sequenciais, conforme apresentado na Figura 4.

Figura 4 - Metodologia de análise do *Energy Expert Cyber Security Platform*



Fonte: EECSP (2017).

O relatório possuía dois objetivos centrais:

- Promover a segurança cibernética dos sistemas energéticos que assegurem a provisão de serviços essenciais à sociedade europeia; e
- Proteger os dados nos sistemas energéticos e assegurar a privacidade dos cidadãos europeus.

Neste sentido, o EECSP procurou responder às seguintes questões:

i. O segmento de energia é diferente de qualquer outro setor no que diz respeito à segurança cibernética?
ii. Quais são os desafios a serem enfrentados no setor de energia?
iii. Quais são as principais áreas estratégicas do setor energético?
iv. Quais são as ações recomendadas em relação à segurança cibernética quando a Diretiva SRI e o GDPR forem totalmente implementados?

Inicialmente, o estudo aponta que, ao contrário do que acontece em outras atividades, no setor energético, a confiabilidade e a resiliência são aspetos muito relevantes, dado que um sistema de controle que seja objeto de um ataque não pode ser facilmente desconectado da rede e pode conduzir a descontinuidades no fornecimento.

Em termos gerais, na segurança cibernética, existem três objetivos centrais:

- Confidencialidade: garantia de que a informação não é divulgada de forma inadequada;
- Integridade: garantia da prevenção contra a modificação ou destruição não autorizada de informação; e

- Disponibilidade: garantia da acessibilidade da informação onde e quando necessária e sem demora indevida.

No setor elétrico, os objetivos prioritários dependem das atividades que são objeto de análise. Na geração e nas redes de transmissão, por exemplo, a disponibilidade e a integridade são centrais, já na medição inteligente (*smart metering*), a confidencialidade dos dados pessoais é o aspeto central. A partir do reconhecimento dessas especificidades, o EECSP identificou dez grandes desafios a serem endereçados no setor:

i. Preservação da estabilidade em uma rede interconectada e transfronteiriça: na Europa, as redes elétricas são fortemente interconectadas, de forma que uma falha em determinado sistema pode provocar um efeito cascata, impactando diversas regiões;

ii. Definição de conceitos de proteção compatíveis com ameaças e riscos correntes: os conceitos de proteção são normalmente estabelecidos no ato de contratação de um sistema, considerando os riscos e as ameaçadas então conhecidos. No entanto, esses vetores evoluem rapidamente, o que pode tornar sistemas e equipamentos incompatíveis com padrões de segurança atualizados;

iii. Gestão de ataques cibernéticos: lidar com ataques cibernéticos e gerenciar todas as fases após um ataque bem-sucedido é uma tarefa complexa para uma variedade de partes interessadas. Os efeitos de ataques cibernéticos não são plenamente considerados na base de concepção do setor elétrico, de modo que os critérios vigentes (a exemplo do critério n-1) podem não ser capazes de garantir a confiabilidade do fornecimento de energia em caso de eventos específicos;

iv. Inserção de novas tecnologias e serviços altamente interconectados: grande atenção aos riscos cibernéticos e às competências para lidar com um ecossistema em constante mudança são demandados com a entrada de novas tecnologias e serviços altamente interconectados;

v. Terceirização de infraestruturas e serviços: a pressão pela redução dos preços da energia no mercado atacadista levou a uma demanda crescente por serviços de dados (por exemplo, baseados em nuvem) e redes de telecomunicações, prestados por outros setores, os quais, não raramente, contam com requisitos menos rigorosos de disponibilidade e integridade. A terceirização de infraestruturas e serviços, portanto, pressupõe a definição de regras de gerenciamento de riscos compatíveis com o setor elétrico;

vi. Integridade dos componentes usados em sistemas energéticos: componentes corrompidos com funções ocultas ou programas *backdoor* são dificilmente detectáveis e caracterizam um grande risco ao setor;

vii. Elevada interdependência entre os participantes do mercado: com o aumento do número de agentes e a crescente aplicação de tecnologias de automação no controle da rede, os riscos à segurança do fornecimento aumentam proporcionalmente, na medida em que uma disrupção na operação pode ser causada por agentes direta ou indiretamente conectados;

viii. Disponibilidade de recursos humanos: a necessidade de lidar com as competências de TIC em um ambiente de tecnologia da operação (TO) leva à crescente demanda por recursos humanos para gerenciar a segurança cibernética. No entanto, esses recursos são escassos, uma vez que os programas de educação atuais estão focados em engenheiros de TIC ou engenheiros elétricos; e

ix. Restrições impostas por medidas de segurança cibernética, em contraste com os requisitos de balanceamento em tempo real e de disponibilidade: as medidas convencionais de segurança cibernética são desenhadas para atender as necessidades de sistemas de tecnologia da informação (TI), o que, muitas vezes, as tornam incompatíveis com sistemas nos quais a disponibilidade e a otimização em tempo real são essenciais à segurança do fornecimento, como o setor elétrico.

Segundo o EECSP, a mitigação desses desafios pressupõe avanços nas seguintes áreas estratégicas:

1. Mapeamento das ameaças e riscos cibernéticos presentes no cenário europeu como ponto de partida para que as ameaças e os riscos ao setor elétrico sejam adequadamente compreendidas e endereçadas;

2. Mapeamento dos operadores de serviços essenciais;

3. Estruturação de um plano de resposta a ataques cibernéticos;

4. Estabelecimento de planos de gerenciamento de crises;

5. Definição e desenvolvimento do grau de maturidade da comunidade europeia em relação à segurança cibernética;

6. Definição de uma estrutura que garanta a integridade da cadeia de valor dos componentes dos sistemas elétricos;

7. Construção de capacidade e competências;

8. Intercâmbio de informações e das melhores práticas relacionadas à segurança cibernética;

9. Promoção da cooperação internacional; e

10. Realização de campanha de sensibilização do alto nível das instituições europeias.

Com base na avaliação estruturada dos desafios e lacunas a serem superadas, o EECSP sistematizou quatro prioridades estratégicas e as relacionou às áreas de ações correspondentes. Para uma análise desta temática, apresenta-se o Quadro 2, a seguir.

Quadro 2 - Relatório EECSP: Prioridades estratégicas e ações recomendadas

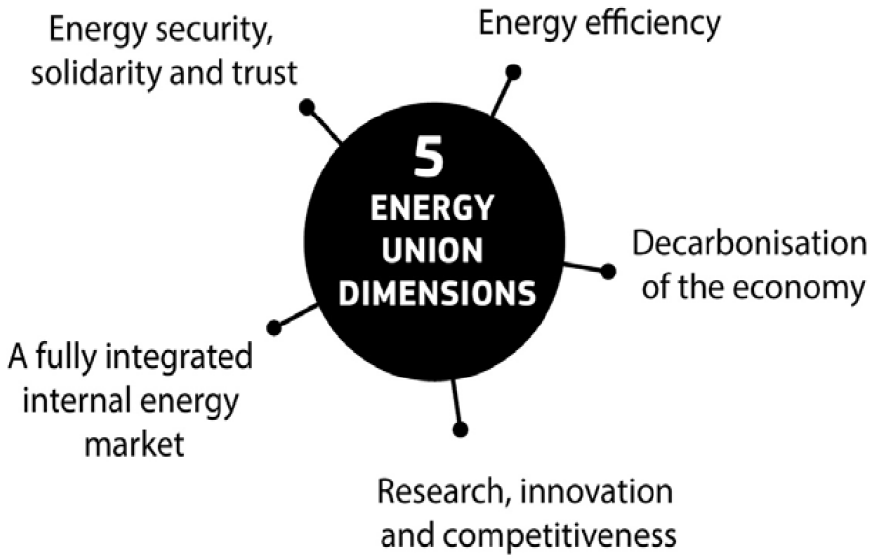
Strategic Priorities		Strategic Areas	Areas of Actions
I	Set-up an effective threat and risk management system	European threat and risk landscape and treatment	(1) Identification of operators of essential services for the energy sector at EU level. (2) Risk analysis and treatment. (3) Framework of rules for a regional cooperation. (4) EU framework for vulnerabilities disclosure for the energy sector.
		Identification of operators of essential services	
		Best practice and information exchange	
		Foster international collaboration	
II	Set-up an effective cyber response framework	Cyber response framework	(5) Define and implement cyber response framework and coordination. (6) Implement and strengthen the regional cooperation for emergency handling
		Crisis management	
III	Continuously improve cyber resilience	European cyber security maturity framework	(7) Establish a European cyber security maturity framework for energy. (8) Establish a cPPP for supply chain integrity (9) Foster European and international collaboration
		Supply chain integrity framework for components	
		Best practice and information exchange	
		Awareness campaign from top level EU institutions	
IV	Build-up the required capacity and competences	Capacity & competence build-up	(10) Capacity and competence build-up.

Fonte: EECSP (2017).

1.3 A segurança cibernética no pacote "*Clean Energy for all Europeans*"

Na sequência do Acordo de Paris, a União Europeia aprovou, em 2019, um pacote legislativo com cinco dimensões estratégicas para a União da Energia (ver Figura 5).

Figura 5 - As cinco dimensões estratégicas da União da Energia



Fonte: Comissão Europeia (2019).

Neste contexto, foram aprovados quatro documentos de grande relevância para a segurança cibernética no âmbito do setor elétrico:

- Diretiva (UE) 2019/944 do Parlamento Europeu e do Conselho da União Europeia, de 5 de junho de 2019, relativa a regras comuns para o mercado interno de eletricidade e que altera a Diretiva 2012/27/EU;
- Regulamento (UE) 2019/943 do Parlamento Europeu e do Conselho da União Europeia, de 5 de junho de 2019, relativo ao mercado interno de eletricidade;
- Recomendação (UE) 2019/553 da Comissão Europeia, de 3 de abril de 2019, sobre a segurança cibernética no setor da energia; e

- Regulamento (UE) 2019/941 do Parlamento Europeu e do Conselho da União Europeia, de 5 de junho de 2019 relativo à preparação para riscos no setor de eletricidade e que revoga a Diretiva 2005/89/CE.

O Quadro 3, a seguir, apresenta um resumo dos objetivos dos documentos produzidos.

Quadro 3 - Regulamentações da Comissão Europeia sobre a segurança cibernética e proteção de dados no setor energético

DIRETIVA (UE) 2019/944 DO PARLAMENTO EUROPEU E DO CONSELHO
REGULAMENTO (UE) 2019/943 DO PARLAMENTO EUROPEU E DO CONSELHO Estabelecem princípios gerais sobre a segurança cibernética e a proteção de dados aplicáveis aos medidores inteligentes e às redes de transmissão e distribuição.
RECOMENDAÇÃO (UE) 2019/553 DA COMISSÃO A recomendação define as principais questões relacionadas à segurança cibernética no setor da energia, nomeadamente os requisitos em tempo real, os efeitos em cascata e a combinação de tecnologias clássicas e de ponta. Identifica, ainda, as principais ações para a aplicação de medidas pertinentes de preparação em matéria de segurança cibernética, no setor da energia. As orientações estão focadas na análise de risco e no grau de prontidão em relação a sistemas, *softwares, hardwares* e sistemas de monitoramento automatizados.
REGULAMENTO (UE) 2019/941 DO PARLAMENTO EUROPEU E DO CONSELHO É um regulamento muito focado na prevenção de crises, que estabelece normas para a cooperação entre os Estados-Membros, tendo em vista a prevenção, a preparação e a gestão de crises de eletricidade, em um espírito de solidariedade e de transparência, e no pleno respeito aos requisitos de um mercado interno de eletricidade competitivo.

Devido à relevância destas quatro regulamentações, o Anexo II destaca as contribuições essenciais de cada uma delas.

2 A SEGURANÇA CIBERNÉTICA NOS PAÍSES DA UNIÃO EUROPEIA

O Conselho de Reguladores de Energia Europeus publicou, em 2019, um relatório intitulado "*Cybersecurity Benchmark*", no qual faz um estudo de *benchmarking* muito detalhado para 16 países da União Europeia. Este estudo, cujas informações dizem respeito a 2018, permitiu elaborar as seguintes conclusões:

- Todos os países aprovaram uma estratégia nacional para a segurança cibernética (vide Quadro 1). No entanto, a grande maioria dos países não dispõe de uma estratégia para a segurança cibernética específica ao sector elétrico;
- Embora respeitando os princípios e as normas estabelecidas na Diretiva SRI, os diferentes países tendem a optar por modelos de governança muito distintos em relação às autoridades nacionais competentes, aos pontos de contato únicos e aos CSIRT com atribuições referentes à segurança das redes e dos sistemas de informação;
- Como discutido na Seção 1, a União Europeia aprovou, no âmbito do pacote legislativo "*Clean Energy for all Europeans*", quatro diplomas de grande relevância para a segurança cibernética e com aplicação específica ao setor elétrico: uma diretiva, dois regulamentos e uma recomendação. Enquanto os regulamentos comunitários são de aplicação direta aos Estados-Membros, as diretivas definem o resultado a alcançar, mas deixam margem aos governos nacionais para legislarem sobre as medidas para concretizarem esses objetivos[1]. A maior parte dos países estabeleceu uma legislação transversal sobre a segurança cibernética, mas optou por

[1] O artigo 288 do Tratado sobre o Funcionamento da União Europeia estabelece que a diretiva vincula os países aos quais se destina quanto ao resultado a alcançar, deixando, no entanto, às instâncias nacionais a competência quanto à forma e aos meios. Contudo, a diretiva é diferente do regulamento ou da decisão. Ao contrário do que acontece com o regulamento, que é imediatamente aplicável na ordem jurídica interna dos países da União Europeia após a sua entrada em vigor, a diretiva não é diretamente aplicável. Para que governos, empresas e particulares possam recorrer a uma diretiva, esta deve ter sido objeto de transposição para o direito nacional.

não definir normas específicas aos diferentes subsetores dos operadores de serviços essenciais e aos prestadores de serviços digitais, considerando que os regulamentos são de aplicação automática. No entanto, a maioria dos países criou agências específicas para alguns setores, como as comunicações, os sistemas de informação ou a energia;

- Na maior parte dos países, o ponto de contato único está sediado na autoridade nacional competente;
- Todos os países publicam um relatório periódico sobre o estado da segurança cibernética;
- Todos os países estabeleceram uma lista de critérios para a definição do operador de serviços essenciais e a maioria dos países já identificou a sua lista de operadores de bens essenciais. Os prestadores de serviços digitais ao setor elétrico, porém, não estão identificados;
- Os operadores de serviços essenciais têm a obrigação de reportar incidentes e, na sua maioria, o reporte é efetuado junto à autoridade nacional competente;
- A grande maioria dos países dispõe de programas universitários especializados em segurança cibernética. Como apresentado anteriormente, na análise do relatório "*Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector*", as insuficiências ao nível das qualificações são uma das principais condicionantes das políticas públicas para a segurança cibernética;
- Quase todos os países atribuem as suas certificações de acordo com a série ISO/IEC; e
- Apenas nove países organizaram "*Systems Risk Assessment*" ao nível nacional para o setor energético.

Em relação aos reguladores da energia ou às empresas reguladas, destacam-se as seguintes conclusões:

- Apenas nove reguladores dispõem de expertise em segurança cibernética;
- Na maior parte dos países, os reguladores de energia não possuem atribuições ao nível da segurança cibernética;
- Na maioria parte dos países, os reguladores são informados sobre incidentes;
- Na grande maioria dos países, as empresas reguladas do setor elétrico organizaram exercícios de simulação de segurança cibernética;
- Na grande maioria dos países, as empresas reguladas estabeleceram padrões de segurança cibernética voluntários;
- Os sistemas de segurança cibernética das empresas reguladas foram objeto de auditorias pelos reguladores setoriais na maioria dos países; e
- Na maior parte dos países, existem plataformas colaborativas para partilha de boas práticas envolvendo empresas e entidades públicas.

3 O PAPEL DOS REGULADORES DE ENERGIA NA SEGURANÇA CIBERNÉTICA

Face à nova legislação europeia sobre a segurança cibernética e a proteção de dados, busca-se identificar, neste capítulo, os novos desafios para os reguladores setoriais europeus ao nível dos marcos regulatórios, na mudança das atitudes e da cultura organizacional dos operadores de bens essenciais e no compartilhamento e na disseminação das boas práticas.

3.1 A sugestão de um papel ativo dos reguladores pela legislação europeia específica para a segurança cibernética no setor elétrico

A legislação europeia sobre segurança cibernética específica para o setor elétrico, apresentada na Seção 1.3, sugere que os reguladores deverão ter um papel ativo nesta matéria (ver Quadro 3).

A Diretiva 2019/944, relativa a regras comuns para o mercado interno de eletricidade, atribui relevância a dois temas em relação aos quais os reguladores europeus possuem, em geral, competências atribuídas, sendo eles:

- Funcionalidades dos sistemas de medidores inteligentes, segurança cibernética e proteção de dados; e
- Funções dos operadores de redes e a segurança cibernética.

O Regulamento 2019/943, relativo ao mercado interno de eletricidade, explicita temas aos quais os reguladores não podem ser alheios, sendo eles:

- Promoção da segurança cibernética nas redes REORT[2] e ORDUE[3] para a eletricidade;
- Promoção da segurança cibernética e da proteção de dados, em cooperação com as autoridades competentes e as entidades regulamentadas; e

[2] REORT – Rede Europeia dos Operadores das Redes de Transporte.
[3] ORDUE - Operadores da Rede de Distribuição da União Europeia.

- Estabelecimento de códigos de rede, ou seja, regulamentos específicos para os diferentes aspetos ligados à segurança cibernética dos fluxos transfronteiriços de eletricidade.

A Recomendação 2019/553, sobre a segurança cibernética na energia, enfatiza três caraterísticas típicas do setor elétrico que podem se refletir na amplificação de efeitos no caso de ocorrerem incidentes, quais sejam:

- Requisitos em tempo real das componentes da infraestrutura energética;
- Efeitos em cascata; e
- Coexistência de tecnologias antigas e de ponta.

Por fim, o Regulamento 2019/941, relativo à preparação para riscos no setor da eletricidade, atribui uma grande relevância à *Agency for the Cooperation of Energy Regulators* (ACER) no acompanhamento e na monitorização das diferentes fases dos procedimentos definidos.

3.2 A perseguição a custos eficientes da promoção da segurança cibernética

A Diretiva SRI estabelece que as medidas técnicas e organizacionais aplicáveis aos operadores de serviços essenciais e aos prestadores de serviços digitais deverão respeitar os seguintes critérios:

- Princípio da neutralidade tecnológica, isto é, não deverão exigir que um determinado produto das tecnologias da informação e da comunicação que tenha fins comerciais seja concebido, desenvolvido ou fabricado de um modo específico; e
- Custo-eficazes, ou seja, deverão prosseguir os objetivos a custos eficientes. Assim, os requisitos estabelecidos deverão ser proporcionais em relação ao risco apresentado pelas redes e pelos sistemas de informação em causa, considerando os progressos técnicos mais recentes no que diz respeito às tecnologias que viabilizam a aplicação de tais medidas.

Os custos decorrentes do reforço da segurança cibernética têm duas componentes, o OPEX associado à prestação de serviços de IT e consultoria e o CAPEX relacionado com a aquisição de software e licenças. Admitindo que os custos decorrentes do reforço da segurança cibernética possam ter um aumento significativo, os reguladores devem ter um papel relevante na promoção de investimentos eficientes nesta área. Destaca-se que, de acordo com um relatório do CEER[4], alguns reguladores, como é o caso do regulador alemão (*Bundesnetzagentur* – BNetzA[5]), definiram padrões mínimos aos requisitos de IT em relação à segurança cibernética.

3.3 A segurança cibernética e o planeamento de redes

Os planos decenais de investimento das redes de transmissão e quinquenais das redes de distribuição são objeto de avaliação e eventual revisão de dois em dois anos. A informação e o conhecimento do regulador setorial sobre temas relacionados à segurança cibernética contribuem, naturalmente, para tornar mais eficaz e eficiente a intervenção dos reguladores nesta matéria.

Para além disso, e como já foi referido, os reguladores europeus têm, em cooperação com o ACER, de contribuir para a elaboração e atualização dos códigos de rede, incluindo aqueles que digam respeito a aspetos relacionados à segurança cibernética.

3.4 Os critérios para a identificação dos operadores de serviços essenciais

Embora admitindo que a maioria dos subsetores da energia já teriam tomado medidas de forma a garantir a segurança cibernética, o grupo de especialistas EECSP recomendou a definição de uma metodologia harmonizada, estruturada

[4] CEER (2018).

[5] Sobre a BNetzA, veja o seguinte link: https://www.bundesnetzagentur.de/EN/Home/home_node.html.

e compreensiva para identificar os operadores de serviços essenciais no setor energético ao nível da União Europeia.

De acordo com o relatório "*Cyber Security Work Stream CEER Cybersecurity Report on Europe's Electricity and Gas Sectors*"[6] do CEER, a definição de regras sobre os operadores de serviços essenciais foi um processo complexo devido à heterogeneidade existente ao longo da cadeia de valor do setor elétrico (geração, transmissão e distribuição).

Um outro aspeto relevante é a definição de sistemas nacionais de certificação que estabeleçam padrões mínimos harmonizados, uma vez que os países já possuem estabelecidos sistemas de certificação distintos. Alguns países, como é o caso da Alemanha, fixaram critérios com base em sistemas de certificação já existentes tal como é o caso da ISO/IEC 27001 e da ISO/IEC 27019.

3.5 A necessidade de institucionalizar uma nova atitude empresarial em relação à segurança cibernética

Destaca-se que o reforço da segurança cibernética no setor elétrico envolve não apenas um aprofundamento dos conhecimentos técnicos, mas também uma mudança de cultura que valorize esta nova dimensão da gestão do setor, tendo em vista o cumprimento da Diretiva SRI. A institucionalização do *Chief Information Security Officer* (CISO), responsável pela segurança cibernética na empresa e reporte para a diretoria, é uma dimensão muito relevante na mudança da cultura organizacional. Naturalmente, esta função deverá estar dotada de recursos adequados e de um mandato claro e transversal a toda a organização.

A adoção de novas soluções de sistemas de informação, como a *cloud computing* ou novos sistemas analíticos de tratamento da *Big Data*, deve ser precedida da explicitação de uma estratégia clara e aprofundada de segurança cibernética por parte dos operadores de rede de transmissão e distribuição, bem como dos

[6] https://www.ceer.eu/documents/104400/-/-/684d4504-b53e-aa46-c7ca-949a3d296124.

fornecedores de tecnologia[7]. Esta estratégia deve, nomeadamente, identificar riscos e medidas de mitigação previamente à decisão de investimento.

Pelo seu conhecimento aprofundado do setor elétrico, entende-se que os reguladores setoriais possuem um papel decisivo a desempenhar nestas matérias, em cooperação com as autoridades nacionais para a segurança cibernética.

3.6 A sensibilização e o compartilhamento de informação e das boas práticas

Os reguladores nacionais devem possuir um posicionamento proativo, consolidando uma cultura organizacional que privilegie a segurança cibernética, de modo a estimular o envolvimento de todos os *stakeholders* no cumprimento da Diretiva SRI e a adotar as melhores práticas internacionais em matérias relacionadas à segurança cibernética.

O *benchmarking* apresentado na Seção 2 mostra que a maioria dos reguladores europeus, muitas vezes em parceria com as autoridades nacionais responsáveis pela segurança cibernética, está envolvida e participa ativamente em plataformas público-privadas que promovem a partilha de informação sobre segurança cibernética. Nesta matéria, merece destaque o regulador esloveno (AGEN[8]), que organiza anualmente um evento internacional, o *Slovene Cyber Secutiry Forum*[9]. Por sua vez, o regulador norueguês também realiza anualmente um *workshop* sobre segurança cibernética em parceria com o ACER e o CEER.

Finalmente, observa-se que a análise de *benchmarking* apresentada na Seção 2 permite concluir que apenas nove reguladores europeus dispõem de expertise em matérias relacionadas à segurança cibernética.

[7] Para uma análise mais detalhada desta questão, veja CEER (2018).

[8] Sobre a AGEN veja o seguinte link: https://www.agen-rs.si/web/en/about-the-agency.

[9] Sobre o Slovene Cyber Secutiry Forum, veja o seguinte link: https://www.infosek.net/en.

4 A SEGURANÇA CIBERNÉTICA EM PORTUGAL

Esta seção apresenta a realidade portuguesa, destacando três temas centrais: o quadro nacional de referência para a segurança cibernética, o enquadramento legislativo e regulatório da segurança cibernética no setor elétrico e, finalmente, o papel do regulador setorial (ERSE) na promoção da segurança cibernética em Portugal.

4.1 O Quadro Nacional de Referência para a Segurança Cibernética

O Quadro Nacional de Referência para a Segurança Cibernética cumpre, naturalmente, os princípios estabelecidos pela Diretiva SRI e possui dois pilares essenciais:

- O regime jurídico da segurança do ciberespaço é estabelecido pela Lei nº 46/2018, que transpôs para o direito interno as normas estabelecidas pela Diretiva SRI 2016/1148; e
- A Estratégia Nacional de Segurança do Ciberespaço, aprovada pela Resolução do Conselho de Ministros nº 92/2019, que possui "*o compromisso de aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa do ciberespaço de interesse nacional e potenciar uma utilização livre, segura e eficiente do mesmo por parte de todos os cidadãos, das empresas e das demais entidades públicas e privadas*"[10].

O Centro Nacional de Segurança Cibernética (CNC)[11] é a Autoridade Nacional de Segurança Cibernética, configurando o ponto de contato único nacional para efeitos de cooperação internacional, e exerce as funções de regulação, regulamentação, supervisão e fiscalização nos termos das suas competências.

[10] Quadro Nacional de Referência para a Segurança Cibernética, Centro Nacional de Segurança Cibernética, 2020, p. 14.
[11] Para mais informações, consulte o Portal do CNC: https://www.cncs.gov.pt/.

O CNC atua em articulação com a Comissão Nacional de Proteção de Dados, quando estejam em causa incidentes que tenham dado origem à violação de dados pessoais.

O CERT.PT, que funciona no CNC, é a Equipe de Resposta a Incidentes de Segurança Informática Nacional[12] e possui as seguintes competências:

- Exercer a coordenação operacional na resposta a incidentes, nomeadamente em articulação com as equipes de resposta a incidentes de segurança informática setoriais existentes;
- Monitorar os incidentes com implicações a nível nacional;
- Ativar mecanismos de alerta rápido;
- Intervir na reação, análise e mitigação de incidentes;
- Proceder a análise dinâmica dos riscos; e
- Assegurar a cooperação com entidades públicas e privadas.

Cabe destacar ainda que o CERT.PT é membro da Rede Nacional de CSIRT e representante na Rede Europeia de CSIRT estabelecida pela Diretiva (EU) 2016/1148.

4.2 O enquadramento legislativo e regulatório da segurança cibernética no setor elétrico

Como já mencionado anteriormente, para além da legislação transversal sobre a segurança cibernética contida na Lei nº 46/2018, devem ainda ser consideradas todas as iniciativas legislativas aprovadas pelo Parlamento Europeu e o Conselho com aplicação específica ao setor elétrico, apresentadas na Seção 1.3 e detalhadas no Anexo II deste trabalho. Ademais, a Diretiva SRI já foi objeto de transposição para o direito interno português e os regulamentos têm aplicação direta e imediata à realidade nacional sem necessidade de transposição.

[12] O CSIRT, na terminologia da Diretiva (EU) 2016/1148.

Observa-se que a identificação dos operadores de serviços essenciais é de responsabilidade do CNC, sendo objeto de atualização anual. Como se pode verificar no Quadro 4, no caso do setor elétrico, os comercializadores e os operadores das redes de transmissão e distribuição são identificados como operadores de serviços essenciais através da Lei nº 46/2018.

Quadro 4 – Extrato da lista dos operadores de serviços essenciais

Setor	Subsetor	Tipo de entidades
Energia	Eletricidade	Empresa de eletricidade que exerce a atividade de comercialização. Operadores da rede de distribuição. Operadores da rede de transporte.
	Petróleo	Operadores de oleodutos de petróleo. Operadores de instalações de produção, refinamento e tratamento, armazenamento e transporte de petróleo.
	Gás	Empresas de comercialização. Operadores da rede de distribuição. Operadores da rede de transporte. Operadores do sistema de armazenamento. Operadores da rede de gás natural em estado líquido (GNL). Empresas de gás natural. Operadores de instalações de refinamento e tratamento de gás natural.

Fonte: Lei nº 46/2018.

Os operadores de serviços essenciais têm a obrigação de reportar incidentes para o CNC, incluindo informações que permitam estimar o impacto transfronteiriço dos mesmos. Neste sentido, a fim de determinar a relevância do impacto de um incidente, são considerados os seguintes parâmetros:

- O número de consumidores afetados;
- A duração do incidente; e
- A distribuição geográfica, no que se refere à região afetada pelo incidente.

Com base na informação prestada na notificação, o CNC informa os pontos de contato únicos dos outros Estados-Membros afetados, caso o incidente tenha um impacto importante na continuidade dos serviços essenciais destes países. Destaca-se que o CNC salvaguarda a segurança e os interesses do operador de serviços essenciais, bem como a confidencialidade da informação prestada na sua notificação.

Sempre que as circunstâncias o permitem, o CNC presta ao notificante as informações relevantes relativas ao seguimento da sua notificação, nomeadamente aquelas que possam contribuir para o tratamento eficaz do incidente.

Após consultar o notificante, o CNC pode divulgar incidentes específicos de acordo com o interesse público, salvaguardando a segurança e os interesses dos operadores de infraestruturas críticas.

Nota-se que a estratégia e as normas para a segurança cibernética são transversais e se aplicam a todos os operadores de serviços essenciais, não existindo uma estratégia ou normas específicas para o setor elétrico. Ademais, as certificações são atribuídas de acordo com a série ISO/IEC270[13].

4.3 O papel da ERSE na promoção da segurança cibernética em Portugal

A análise do comportamento da ERSE em relação à segurança cibernética é baseada na seguinte documentação:

- O relatório de *benchmark* do CEER com o título "*Cybersecurity Benchmark*"[14];
- Os Relatórios de Atividades e Contas da ERSE de 2018[15] e 2019[16] e a Lei nº 46/2018; e
- O Protocolo assinado entre a ERSE e o Gabinete Nacional de Segurança/Centro Nacional de Segurança Cibernética[17].

[13] Sobre os sistemas de certificação, recomenda-se consultar o documento subordinado ao título "Quadro Nacional de Referência para a Segurança Cibernética, Centro Nacional de Segurança Cibernética", de 2020.

[14] Ver: https://www.ceer.eu/documents/104400/-/-/f301a06f-2224-353f-fed9-eee50a10d78d.

[15] Ver: https://www.erse.pt/media/vn1oi0c3/rac-2018.pdf.

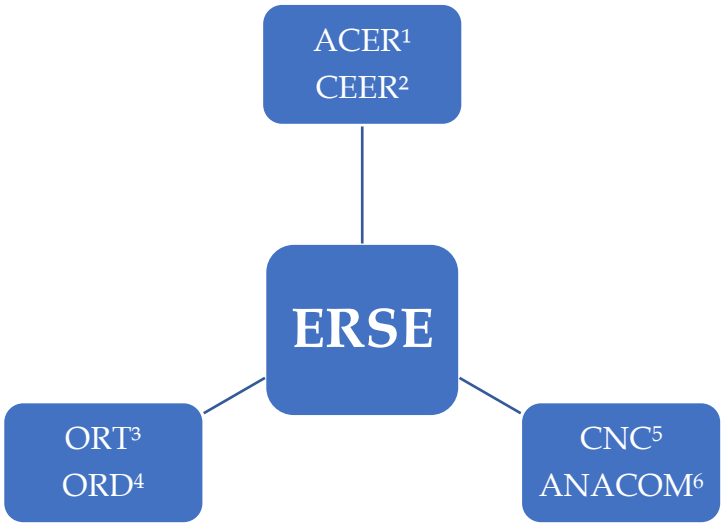
[16] Ver: https://www.erse.pt/media/ymfjwf31/rac_2019.pdf.

[17] Ver: https://www.erse.pt/media/vccd1rvt/cncs_13042016.pdf

Face à transversalidade da segurança cibernética, a ERSE tem desenvolvido uma estratégia colaborativa em rede com diferentes instituições, conforme apresentado na Figura 6:

- Em termos internacionais, a ERSE tem cooperado com o ACER e o CEER, sendo um dos reguladores que participa no grupo de trabalho sobre a segurança cibernética do CEER;
- Em termos nacionais, o regulador português desenvolve atividades conjuntas com o CNC na sequência de um Protocolo de Cooperação estabelecido com esta instituição;
- No que diz respeito à sua atividade de regulação das redes de transmissão e distribuição, a ERSE tem contribuído para a realização eficiente de investimento na segurança cibernética e na proteção de dados, para o cumprimento da Diretiva SRI por parte das empresas reguladas, bem como para a valorização e consolidação de uma nova atitude e cultura empresarial em relação à segurança cibernética.

Figura 6 - Estratégia colaborativa da ERSE em relação à segurança cibernética



Fonte: Elaboração própria

Notas:
[1] Regulador Europeu; [2] Conselho de Reguladores Europeus de Energia;
[3] Operador de Rede de Transmissão; [4] Operador de Rede de Distribuição;
[5] Centro Nacional de Segurança Cibernética; e [6] ANACOM – Regulador Português das Comunicações.

A ERSE e o Gabinete Nacional de Segurança/Centro Nacional de Segurança assinaram um Protocolo de Cooperação em 13 de abril de 2016, quando a Diretiva SRI não estava ainda aprovada e apenas se conhecia uma proposta[18], de forma a potencializar o trabalho conjunto de duas entidades relevantes para a transposição e posterior aplicação da diretiva ao nível nacional. À época, foram selecionadas as seguintes áreas de cooperação:

- Desenvolvimento estratégico;
- Operações de segurança;
- Formação e qualificação de recursos humanos;
- Sensibilização em matéria de segurança cibernética;
- Políticas de segurança cibernética;
- Exercícios de segurança cibernética; e
- Apresentação de candidaturas a projetos com cofinanciamento comunitário.

A análise do exercício de *benchmarking* europeu sobre a segurança cibernética promovido pelo CEER permite constatar que a ERSE é um dos reguladores mais proativos no seu aprofundamento e consolidação, na medida em que foi um dos 16 reguladores participantes. Para além disso, a ERSE apresenta um posicionamento proativo em termos regulatórios, de forma a criar uma nova cultura empresarial, e no compartilhamento de informação em relação a boas práticas na segurança cibernética.

[18] A Diretiva SRI foi publicada a 6 de julho de 2016.

A análise dos Relatórios de Atividades e Contas de 2018 e 2019 da ERSE permite identificar as seguintes inciativas:

- Cooperação com instituições internacionais:
  a) Acompanhamento das questões de segurança cibernética nas redes elétricas, através da participação no grupo de trabalho do CEER; e
  b) Participação no Estudo de *Benchmarking* do CEER sobre a segurança cibernética.
- Cooperação com instituições nacionais:
  a) Participação nas reuniões do Setor de Energia, do Centro Nacional de Segurança Cibernética, no âmbito da Diretiva (UE) nº 2016/1148 (NIS/SRI), relativa à definição de medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação;
  b) Participação no grupo de trabalho para desenvolvimento de atividades de identificação de operadores de serviços essenciais no setor da energia e regulamentação da Lei nº 46/2018 (Centro Nacional de Segurança Cibernética); e
  c) Cooperação com a ANACOM e com a DGEG no âmbito das atividades de interesse comum do setor energético e das telecomunicações.
- Participação em Exercícios de Segurança Cibernética:
  a) Exercício Nacional de Segurança Cibernética 2018 e 2019, promovido pelo Centro Nacional de Segurança Cibernética; e
  b) Exercício Ciberperseu 2018 e 2019, realizado pelo Exército Português.
- Outras ações:
  a) Realização de sessões de consciencialização a todos os colaboradores na área de Segurança de Informação;
  b) Definição das Políticas de Segurança Setoriais, no âmbito da Política Geral de Segurança da Informação da ERSE; e
  c) Ações relacionadas ao Regulamento Geral de Proteção de Dados.

5 AS FRAGILIDADES NAS COMPETÊNCIAS EM SEGURANÇA CIBERNÉTICA NA UNIÃO EUROPEIA E ESTRATÉGIAS DE SUPERAÇÃO

A aprovação da Diretiva SRI sobre a segurança cibernética e do Regulamento GDPR sobre a proteção de dados, em 2016, apresentou reflexos expressivos para os operadores de serviços essenciais e para os prestadores de serviços digitais ao nível da União Europeia. Face a este contexto, a ENISA promoveu um estudo, em 2019, subordinado ao título "*Cybersecurity Skills Development in the EU*".

Este estudo concluiu que, não só na União Europeia, mas também à escala global, existia uma insuficiente quantidade de profissionais qualificados face à procura crescente destas competências. Para além disso, os sistemas de ensino e formação não apresentavam um nível de qualidade apropriado e as atividades de P&D em segurança cibernética estavam muito aquém das necessidades emergentes no contexto atual.

A ENISA (2019) aponta que, em 2019, se verificavam as seguintes condições no segmento da segurança cibernética nos Estados Unidos:

- As vagas de emprego em segurança cibernética aumentaram 94% desde 2013, enquanto as vagas em tecnologia da informação aumentaram apenas 30%;
- Os postos de trabalho relacionados à segurança cibernética responderam por 13% de todos os empregos de TI, mas seus salários comandavam um prêmio de 16% sobre os demais salários na área;
- As vagas de segurança cibernética levaram 20% a mais de tempo para serem preenchidas em relação a outras ocupações em TI; e
- A proporção de profissionais de segurança cibernética empregados, em 2019, em relação ao número de vagas não mudou desde 2015-2016, ficando estável em 2,3, enquanto havia 5,8 trabalhadores empregados para qualquer outro emprego na economia.

Em relação à União Europeia, a ENISA (2019) aponta, a título ilustrativo, os seguintes gargalos:

- Apesar da disponibilidade de quase 500 cursos universitários e de treinamento em toda a Europa, a lacuna de habilidades em segurança cibernética em todos os setores continua sendo um grande desafio e o *pool* de talentos não está acompanhando o ritmo da demanda por profissionais no ramo;
- Havia uma carência de, aproximadamente, 291.000 profissionais de segurança cibernética na Europa, em 2019;
- 33% dos 1.125 diretores de segurança da informação nos Estados Unidos e na UE têm dificuldade em contratar novos talentos e 49% acreditam que isso pode expor suas organizações a riscos maiores; e
- Os profissionais de TI na Alemanha, França, Reino Unido e em todo o mundo estão convencidos de que a escassez de pessoal de segurança cibernética deve perdurar, pois preveem que cerca de 16% das vagas de segurança cibernética podem ficar vagas até 2020.

Estes dados são alarmantes. As diretivas dos diferentes Estados-Membros da União Europeia e a aplicação dos novos regulamentos europeus em segurança cibernética suscitaram a contratação de um número muito expressivo de técnicos, contudo, no mercado de trabalho dos diferentes países, não existiam profissionais em quantidade e nível de qualificações adequados para responderem às novas exigências regulamentares.

Como sugere o estudo da ENISA, dois elementos que agravam a escassez de mão-de-obra podem ser atribuídos aos empregadores ou, de modo mais geral, ao mercado de trabalho. O primeiro é a grande expectativa que os empregadores têm sobre o nível de qualificação dos candidatos que o mercado de trabalho atual pode oferecer, enquanto o segundo é a falta de treinamento suficiente e adequado para os funcionários.

Contudo, há, também, problemas identificados na oferta de qualificações por parte do sistema de educação, formação e P&D. Face aos desajustes entre a

demanda e a oferta de qualificações em segurança cibernética, o sistema de ensino e formação reagiu com uma oferta alargada de cursos (quase 500 cursos), os quais, no entanto, na maioria dos casos, não têm a qualidade exigida. Por isso, a certificação dos currículos destes cursos é um tema muito relevante, tornando-se objeto de iniciativas da União Europeia.

Em 2017, o EECSP identificou, através do estudo "*Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector*", apresentado na Seção 1.2 deste trabalho, a fragilidade existente na formação de recursos humanos e em P&D sobre segurança cibernética. Em matéria de competências, o estudo recomenda que a Comissão Europeia, juntamente com a ACER e a ENISA:

a. Desenvolva uma abordagem sistemática (programa de certificação para currículos técnicos específicos) para alavancar a capacidade e as competências em segurança cibernética no setor de energia;
b. Promova um programa de conscientização multinível (com abordagem *top down*) para a segurança cibernética no setor de energia; e
c. Apoie a construção de uma rede de parceiros para fornecer treinamento e estabelecer e operar programas de certificação e educação com currículos acadêmicos.

A CEER (2019) reitera um ponto identificado pela ENISA: por um lado, existe uma oferta diversificada de formação em segurança cibernética em quase todos os países analisados, mas, por outro lado, alguns reguladores europeus não dispõem de competências nesta matéria. Face à identificação deste *gap*, têm sido desenvolvidas várias iniciativas, apresentadas a seguir, que visam superar esta limitação.

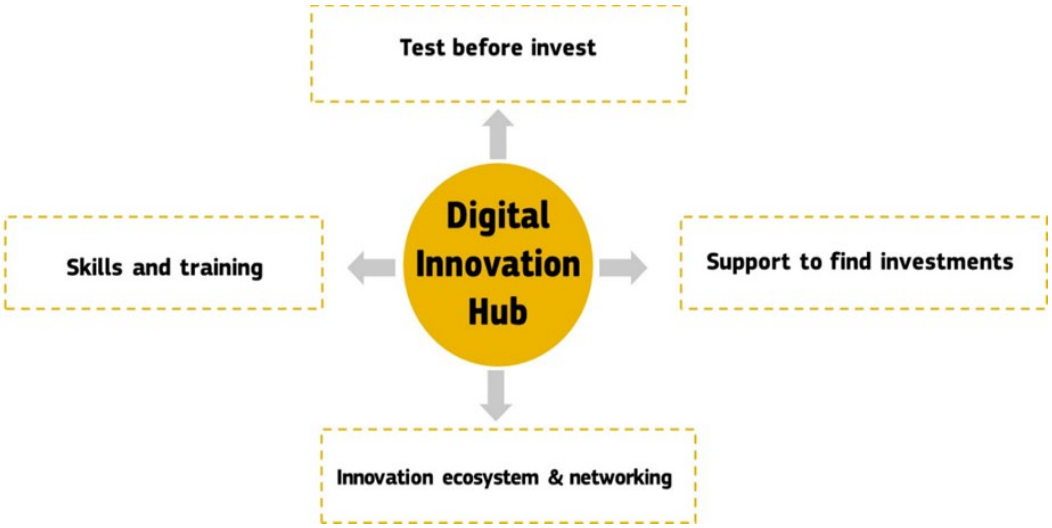
5.1 Os modelos institucionais e organizacionais para o sistema de ensino, formação e inovação em segurança cibernética

Neste ponto, serão analisados os modelos de governança adotados nas instituições utilizadas pela União Europeia como instrumentos para o desenvolvimento de ensino, formação e inovação em segurança cibernética.

5.1.1 Os *Digital Innovation Hubs* (DIHs)

Os DIHs (Figura 7) são uma das prioridades da iniciativa "*Digitising European Industry*", adotada em abril de 2016, com um papel central no Programa "*Digital Europe*", no novo ciclo de financiamento comunitário. De acordo com a Comissão Europeia, os DIHs contribuem para que as empresas se tornem mais competitivas através da aplicação de tecnologias digitais. Assim, os DIHs fornecem acesso à experiência técnica e à experimentação, para que as empresas possam "testar antes de investir". Os *Hubs* também fornecem serviços de inovação, como aconselhamento financeiro, treinamento e desenvolvimento de habilidades, que são necessários para uma transformação digital bem-sucedida (EC, 2021).

Figura 7 – DIH: Modelo de negócios



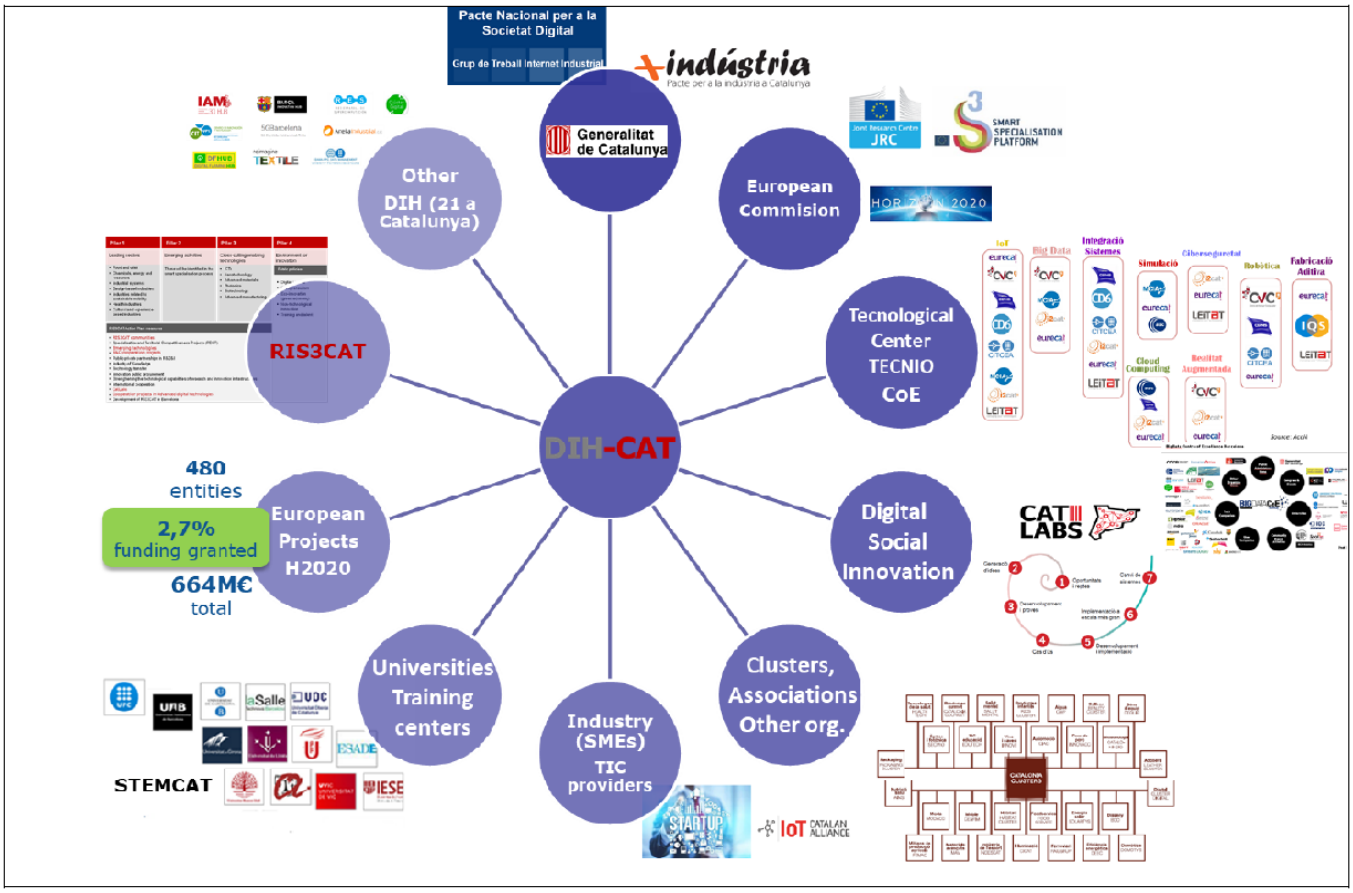
Fonte: Comissão Europeia (2021).

Os DIHs são centros de competência que promovem a cooperação regional de múltiplos parceiros, incluindo organizações como centros tecnológicos, centros

de pesquisa, Universidades, associações industriais, câmaras de comércio, incubadoras/aceleradoras, agências de desenvolvimento regional e, até mesmo, entidades governamentais. Estas entidades devem privilegiar uma relação de parceria com prestadores de serviços fora de sua região, apoiando empresas com acesso aos seus serviços.

A relação estabelecida entre os DIHs e os seus potenciais clientes (Figura 8) é sempre baseada na proximidade existente entre as duas partes. Apresentam-se, em seguida, alguns estudos de caso de DIHs focados na área temática da segurança cibernética e financiados por esta iniciativa comunitária.

Figura 8 – DIH: Ecossistema



Fonte: Rissola *et al.* (2018).

5.1.2 A criação de *Cybersecurity Innovation Hub* na Europa

No contexto da iniciativa DIH, têm sido criados, na Europa, centros de competência em segurança cibernética. Apresentam-se, no Quadro 5, alguns estudos de caso. Já no Quadro 6, identifica-se uma tipologia típica das parcerias destes centros de competência.

Quadro 5 – Estudos de caso

Cybersecurity Innovation Hub República Tcheca https://www.cybersecuritydih.cz/	*Cybersecurity Innovation Hub* Castilla y León, Espanha https://www.cyberdih.com/en/
Cybersecurity Innovation Hub Eslovênia https://www.cybersecurityintelligence.com/digital-innovation-hub-slovenia-dih-4636.html	*Cybersecurity Innovation Hub* Croácia https://www.icent.hr/en/CybersecRDI/
Cybersecurity Innovation Hub Polônia https://cybersechub.eu/	

Fonte: Elaboração própria.

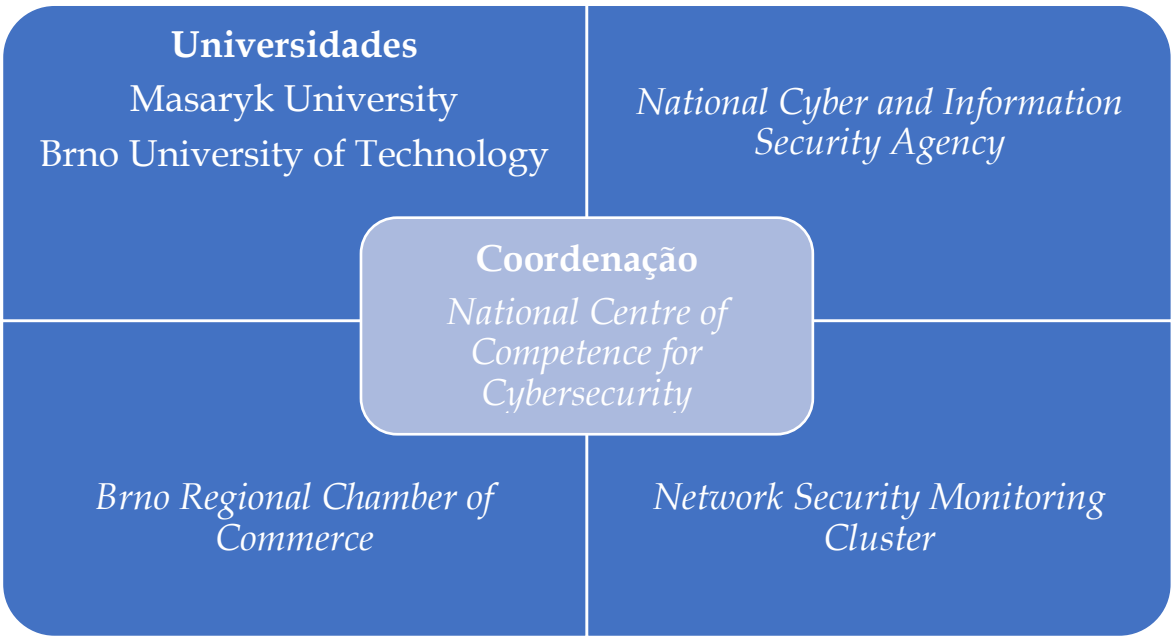
Quadro 6 – Parcerias

- Autoridade Nacional para a Segurança Cibernética;
- Universidades e instituições de P&D;
- Parques de Ciência e Tecnologia;
- Centros de competência e laboratórios;
- Agências de desenvolvimento;
- Empresas de tecnologia e sistemas de informação; e
- Associações empresariais.

Fonte: Elaboração própria.

A Figura 9 apresenta, a título ilustrativo, os membros do *Cybersecurity Innovation Hub* da Eslovênia. Como é possível verificar, os membros incluem a Autoridade Nacional para a Segurança Cibernética, Universidades e Associações Empresariais.

Figura 9 - Membros do *Cybersecurity Innovation Hub* da Eslovênia



Fonte: Elaboração própria.

Nos mesmos moldes, situa-se o *Azores Digital Innovation Hub* (Portugal), que desenvolve atividades em segurança cibernética com o apoio do INESC TEC, um centro de pesquisa especializado em temas relacionados à energia.

5.2 Os centros de excelência para promover a educação e a P&D em segurança cibernética

Conforme mencionado, a ENISA (2019) assinala que, não só na União Europeia, mas também à escala global, existia uma insuficiente quantidade de profissionais qualificados na área de segurança cibernética. Face a esse diagnóstico e às recomendações da Agência, a Comissão Europeia tomou várias iniciativas, entre as quais se destaca o desenvolvimento de quatro projetos piloto — CONCORDIA, ECHO, SPARTA e CyberSec4Europe (Figura 10) —, que visam estabelecer centros de excelência com o objetivo de elaborar um *roadmap* para a consolidação de um sistema comum europeu de pesquisa e inovação para a segurança cibernética.

Figura 10 - Centros de excelência para a segurança cibernética

Fonte: Comissão Europeia (2018).

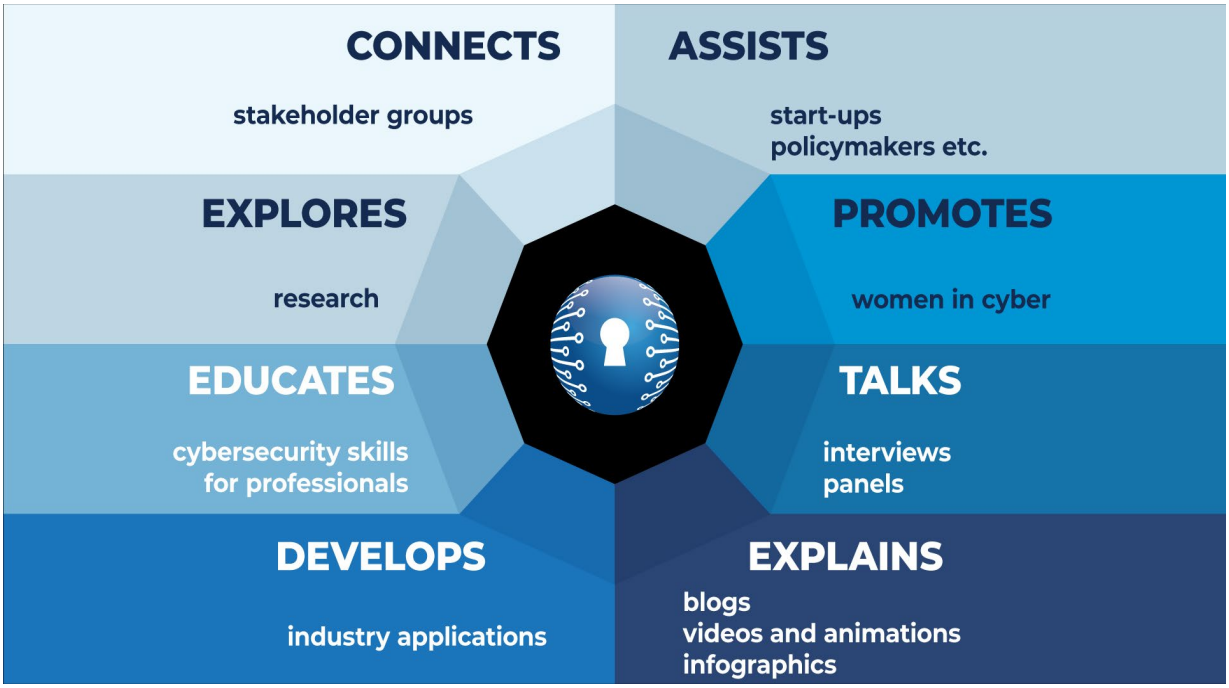
Um dos aspetos marcantes destes centros de excelência é a sua elevada transversalidade temática e geográfica, bem como ao nível das parcerias e dos modelos organizacionais. Estas instituições possuem uma visão e um domínio de intervenção transversal e sistémico da segurança cibernética e, portanto, não são necessariamente especializadas em abordagens setoriais.

Deve-se sublinhar que estas quatro instituições, embora tenham uma preocupação comum e modelos organizacionais tendencialmente semelhantes, possuem objetivos e oferecem produtos, serviços e soluções distintos.

A título ilustrativo, as Figuras 11 e 12 permitem perceber imediatamente o "modelo de negócio", os objetivos e as parcerias da CONCORDIA. Como já mencionado anteriormente, estas quatro entidades valorizam o papel da rede de parceiros, que, no caso da CONCORDIA, é constituída por 52 agentes, provenientes da Academia, Indústria, pequenas e médias empresas, dentre outras organizações, de 20 países europeus.

Dois objetivos muito relevantes destas entidades estão relacionados à formatação e certificação de programas de formação especializada ao nível da graduação e pós-graduação, bem como à definição de uma estratégia de P&D em segurança cibernética. Por exemplo, a SPARTA está trabalhando em projetos interessantes neste domínio, que envolvem mais de 80 programas desenvolvidos por universidades em escala global[19].

Figura 11 - CONCORDIA: Principais motivações e atividades



Fonte: Comissão Europeia (2019).

[19] Sobre esta matéria, consulte o seguinte link: https://www.sparta.eu/training/.

Figura 12 - CONCORDIA: Ecossistema

Fonte: Comissão Europeia (2019).

5.3 A *EU Cyber Academia and Innovation Hub* (EU CAIH)

O EU CAIH é um centro de excelência da União Europeia para a educação e treinamento em segurança cibernética e ciberdefesa, coordenado por Portugal e sediado em Lisboa, que se inspira, simultaneamente, no conceito de DIH e nos centros de excelência.

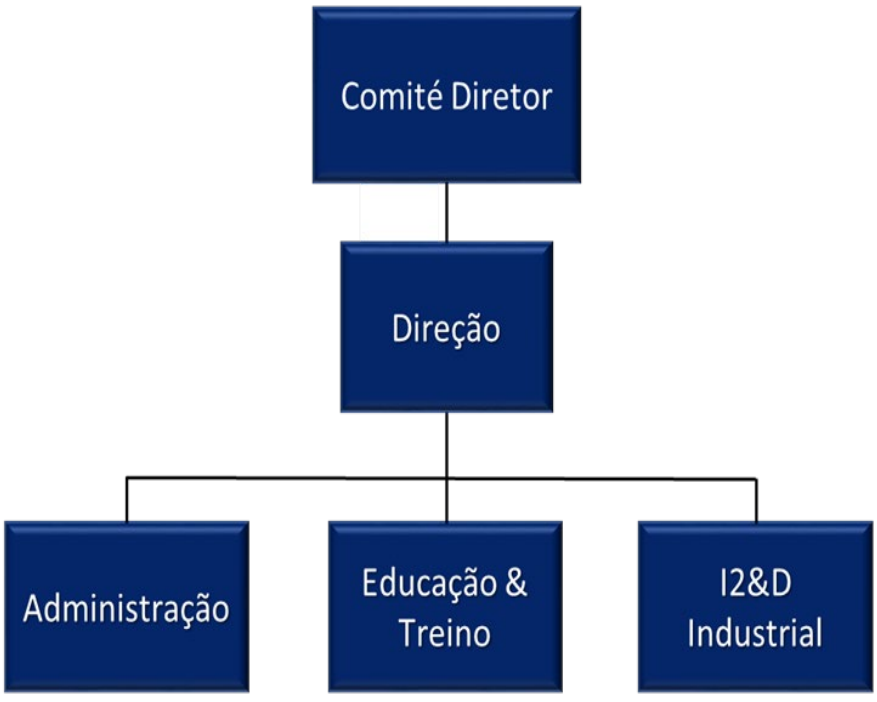
O EU CAIH insere-se no contexto das instituições de referência da *Permanent Structured Cooperation* (PESCO), que fazem parte da política de segurança e defesa

da União Europeia, na qual 25 das 27 forças armadas nacionais visam realizar uma integração estrutural.

Trata-se de um projeto coordenado por Portugal, que envolve a Espanha, como Estado-Membro participante, conta, ainda, como observadores, com Holanda, Polónia e Itália e, como partes interessadas, com França, Grécia e Lituânia.

De acordo com seus promotores, pretende-se que o CAIH seja um centro de excelência, de nível internacional, de ciberdefesa e segurança cibernética, que interligue Universidades, centros de investigação, indústria e outras entidades do setor público e privado, tendo como linhas estratégicas de ação: (i) educação, treino e exercícios; (ii) apoio à investigação, ao desenvolvimento e à inovação; e (iii) apoio ao desenvolvimento da indústria. Definiram-se, ainda, os seguintes domínios prioritários: (i) plataforma de compartilhamento de informações sobre ameaças cibernéticas e resposta a incidentes; (ii) equipes de resposta cibernética rápida e assistência mútua em segurança cibernética; e (iii) centro de coordenação dos domínios cibernéticos e informacionais.

Figura 13 - Estrutura organizacional do EU CAIH



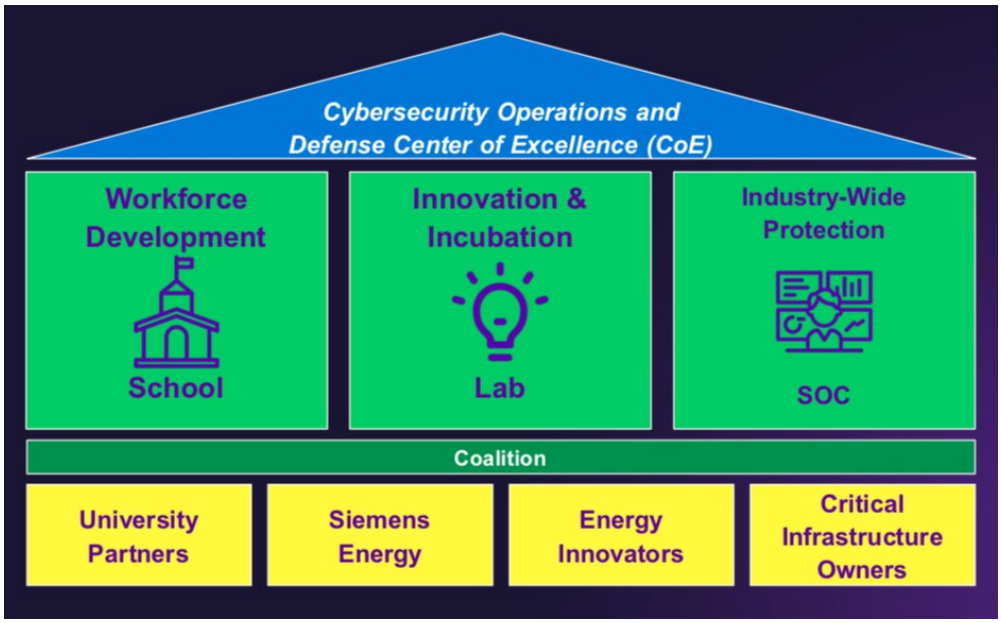
Fonte: Elaboração própria.

5.4 O modelo de centro de excelência a ser implementado no Brasil

A SIEMENS, dentro de uma visão global de centros de excelência em segurança cibernética, está planejando a implantação de um de seus centros no Brasil, com grande ênfase no setor elétrico.

Os fundamentos para esta iniciativa estão em linha com aquelas desenvolvidas na Comunidade Europeia. A Figura 14 apresenta o modelo básico do centro, com destaque para o modelo de participação que propõe uma estrutura de coalizão, incluindo o setor acadêmico, empresas inovadoras na área de novos produtos, inclusive *startups*, operadores de estruturas críticas e a SIEMENS.

Figura 14 – Estrutura básica do centro de excelência



Fonte: Siemens (2020).

Destacam-se, no modelo, os seguintes ambientes: escola, laboratório e Centro de Supervisão de Segurança Cibernética (SOC). A Quadro 7 apresenta cada ambiente, com suas finalidades, requisitos e conceitos básicos adotados.

Quadro 7 – Ambientes do centro de excelência em segurança cibernética

Ambientes	Finalidades	Requisitos	Conceitos Básicos
Escola	Formar mão de obra especializada em segurança cibernética.	- Certificação de parceiros (ex. Universidades); - Estabelecimento de parcerias nas áreas de pesquisas e educação; - Estabelecimento de parcerias na área de tecnologia e simulação (Ex. SIEMENS Energy); e - Obtenção de recursos para elaboração de currículos de treinamento.	Nivelamento dos parceiros para desenvolver iniciativas e modelos de segurança cibernética, através: • Do desenvolvimento de grade curricular para executivos e analistas de segurança cibernética; • De níveis de certificações desejados; e • Do estabelecimento de vínculos de cooperação desejados. O centro de excelência deverá desenvolver e suportar processos de educação formal para as equipes de empresas. Os participantes das iniciativas de treinamento deverão utilizar recursos do laboratório no treinamento.
Laboratório	Suprir a lacuna para testar, certificar e aprimorar soluções de segurança cibernética, principalmente em ambientes operativos. Promover o desenvolvimento de novas expertises e produtos.	- Desenvolvimento de parcerias em tecnologia e simulação; - Obtenção de recursos para montagem de plataforma de testes e processos de certificação; e - Gestão para ampliar as soluções para novas organizações.	Um laboratório para aprovar e expandir soluções para a comunidade de empresas operadoras de infraestrutura crítica, especialmente do setor elétrico. O laboratório deverá abrigar *startups* e outros fornecedores no processo de transformar protótipos em produtos (principalmente na etapa de testes) e *roll out* de novos produtos. O laboratório deverá apoiar processos de certificações.
Centro de Supervisão de Segurança Cibernética	suprir a ausência de um centro para supervisionar recursos de diversos tipos de usuários e para responder a incidentes de segurança cibernética.	- Obter recursos para construir o SOC e para viabilizar e manter a sua equipe; e - Montar uma equipe de analistas e lideranças em segurança cibernética (eventualmente compartilhando-os com a Escola).	O SOC se propõe a gerenciar riscos, supervisionar potenciais ameaças, bem como responder e investigar incidentes da rede operativa e corporativa. Implementação de rede de cooperação com outros SOC.

Fonte: Elaboração própria.

6 CONCLUSÕES

A transição energética e a descarbonização da economia determinaram uma aceleração crescente da digitalização do setor elétrico, o que, considerando a emergência dos ataques cibernéticos, suscitou a necessidade de reforçar a legislação sobre segurança cibernética e proteção de dados.

A aprovação e o avanço da regulamentação da segurança cibernética ao nível da União Europeia, de modo geral, e em Portugal, de forma específica, apresentaram reflexos expressivos nos chamados operadores de serviços essenciais e, também, nos prestadores de serviços digitais.

A evidência empírica disponível em estudos de referência analisados permite concluir que, na União Europeia, mas também à escala global, existe atualmente uma insuficiente quantidade de profissionais qualificados, face à procura crescente destas competências. Além disso, nota-se que os sistemas de ensino, formação e P&D em segurança cibernética estão muito aquém das necessidades emergentes no contexto atual.

Tendo em vista as insuficiências identificadas em P&D sobre segurança cibernética, as instâncias de decisão da União Europeia estabeleceram uma agenda integrando iniciativas que visavam superar as referidas fragilidades, que aposta no envolvimento da indústria em parcerias público-privadas, na promoção de projetos com base nos princípios da neutralidade setorial e tecnológica e na maximização do potencial de replicação das tecnologias e soluções.

A Comissão Europeia desenvolveu soluções institucionais que buscam assegurar uma oferta qualificada de ensino, formação e P&D. Os *Cybersecurity Innovation Hubs* são centros de competência que promovem a cooperação regional de múltiplos parceiros, incluindo a Autoridade Nacional para a Segurança Cibernética, Universidades e instituições de P&D, parques de ciência e tecnologia, centros de competência e laboratórios, agências de desenvolvimento, empresas de tecnologia e sistemas de informação e associações empresariais.

A Comissão Europeia financiou, ainda, o desenvolvimento de quatro projetos piloto - CONCORDIA, ECHO, SPARTA e CyberSec4Europe -, que visam estabelecer centros de excelência com o objetivo de definir um *roadmap* para a consolidação de um sistema comum europeu de pesquisa e inovação.

Considera-se que a experiência reportada poderá servir de modelo a ser estudado pelo Brasil e, principalmente, pelo setor elétrico nacional, com a finalidade de consolidar um arcabouço regulatório para a área de segurança cibernética.

REFERÊNCIAS

CEER, Council of European Energy Regulators (2018). Cybersecurity Report on Europe's Electricity and Gas Sectors. Disponível em: https://www.ceer.eu/documents/104400/-/-/684d4504-b53e-aa46-c7ca-949a3d296124.

CEER, Council of European Energy Regulators (2019). Cybersecurity Benchmark. Disponível em: https://www.ceer.eu/documents/104400/-/-/f301a06f-2224-353f-fed9-eee50a10d78d

CNC, Centro Nacional de Segurança Cibernética (2020). Quadro Nacional de Referência para a Segurança Cibernética. Disponível em: https://www.cncs.gov.pt/content/files/cncs_qnrcs_2019.pdf

Comissão Europeia (2004). Communication from the commission to the council and the European parliament. Critical Infrastructure Protection in the fight against terrorism COM (2004) 702 final. Tech. rep. (2004).

Comissão Europeia (2013). EU Cyber Security Strategy - Estratégia para a Segurança Cibernética na União Europeia. JOIN (2013) 1 final. Disponível em: http://www.eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

Comissão Europeia (2015). Digital Single Market Strategy. Estratégia para o Mercado Único Digital na Europa – COM/2015/0192 final. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

Comissão Europeia (2015). European Agenda on Security – Agenda para a Segurança Europeia. COM (2015) 185 final. Disponível em: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

Comissão Europeia (2016). Digital Innovation Hubs (DIHs) in Europe, shaping Europe's digital future. Disponível em: https://ec.europa.eu/digital-single-market/en/digital-innovation-hubs-dihs-europe

Comissão Europeia (2019). Clean energy for all Europeans, European Commission. Disponível em: https://op.europa.eu/en/publication-detail/-/publication/b4e46873-7528-11e9-9f05-01aa75ed71a1/

Comissão Europeia (2019). Recomendação (UE) 2019/553, de 3 de abril de 2019. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019H0553&from=EN

ECS, European Cyber Security Organization (2016). European Cybersecurity Strategic Research and Innovation Agenda for a Contractual Public-Private Partnership. Disponível em: http://www.ecs-org.eu/documents/ecs-cppp-sria.pdf

EECSP, Energy Expert Cyber Security Platform (2017). Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector. European Commission. Disponível em: https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

ENISA, European Union Agency for Network and Information Security (2019). Cybersecurity skills development in the EU, The certification of cybersecurity degrees and ENISA's Higher Education Database. Disponível em: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

ERSE, Entidade Reguladora dos Serviços Energéticos (2018). Relatório de Atividades e Contas - 2018. Disponível em: https://www.erse.pt/media/vn1oi0c3/rac-2018.pdf

ERSE, Entidade Reguladora dos Serviços Energéticos (2019). Relatório de Atividades e Contas - 2019. Disponível em: https://www.erse.pt/media/ymfjwf31/rac_2019.pdf

ERSE, Entidade Reguladora dos Serviços Energéticos; GNS/CNC, Gabinete Nacional de Segurança / Centro Nacional de Cibersegurança (2016). Protocolo de Cooperação entre o GNS/CNC e a ERSE. Disponível em: https://www.erse.pt/media/vccd1rvt/cncs_13042016.pdf

ISO/IEC 27001. Disponível em: https://www.iso.org/isoiec-27001-information-security.html

ISO/IEC 27019. Disponível em: https://www.iso.org/standard/68091.html

Parlamento Europeu (2019). Cybersecurity of critical energy infrastructure. European Parliament.

RISSOLA, G. *et al* (2018). Digital Innovation Hubs in smart specialization strategies: Early lessons from European regions. European Commission. Disponível em: https://s3platform.jrc.ec.europa.eu/documents/20182/201464/Digital+Innovation+Hubs+in+Smart+Specialisation+Strategies/7a3ed807-de76-4d6a-a698-8363efc03245

União da Energia (2015). Disponível em: https://www.consilium.europa.eu/pt/policies/energy-union/

União Europeia (2016). Diretiva (EU) 2016/1148, de 6 de julho de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L1148&from=EN

União Europeia (2019). Diretiva (UE) 2019/944, de 5 de junho de 2019. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019L0944&from=EN

União Europeia (2016). Regulamento (UE) 2016/679, de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679

União Europeia (2019). Regulamento (EU) 2019/881, de 17 de abril de 2019. Cybersecurity Act. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0881&from=EN

União Europeia (2019). Regulamento (UE) 2019/941, de 5 de junho de 2019. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0941&from=EN

União Europeia (2019). Regulamento (UE) 2019/943, de 5 de junho de 2019. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0943&from=EN

ANEXO I – LISTA ILUSTRATIVA DE INCIDENTES DE ELEVADO IMPACTO

Notable incidents related to physical and cybersecurity of energy

Reports of hackers penetrating Russian and US power networks, 2019
In March 2019, the US grid regulator NERC reportedly warned that a hacking group with suspected Russian ties was conducting reconnaissance into the networks of American electrical utilities. In June 2019, the *New York Times* reported that American 'code' had been deployed inside many elements of Russia's power network by US military hackers that were targeting Russian power plants. The claims were denied by President Trump and regarded with scepticism by cybersecurity experts.

Cyber-attack on petrochemical plant, Saudi Arabia, August 2017
In August 2017, a sophisticated cyber-attack on a Saudi petrochemical plant was the first known attempt to manipulate an emergency shutdown system. The attack resulted in the plant shutting down, but experts warned that it had the potential to cause a serious industrial accident. Cybersecurity experts attributed the incident to a Russian government-owned laboratory.

Cyber-attacks on Ukrainian power grid, 2015 and 2016
The Ukrainian grid suffered two blackouts as a result of cyber-attacks. In December 2015, hackers penetrated the computer system of a western Ukrainian power utility, and cut off the electricity to some 225 000 people. A year later, in December 2016, a cyber-attack disabled an electricity substation and left customers in parts of Kiev without power for about an hour. Both attacks were attributed to Russian hacker groups. Some security researchers suspect that the second attack was intended to cause physical damage to the components of the Ukrainian electricity grid.

Metcalf sniper attack, California, 2013
In April 2013, attackers physically damaged and disabled the Metcalf substation that supplies electricity to Silicon Valley. In a well-planned night-time operation, they cut communication cables and used rifles to severely damage 17 electricity transformers, resulting in damage worth US$15 million. The attackers were not identified and their motivation is not known.

Baku-Tbilisi-Ceyhan oil pipeline explosion, Turkey, 2008
The Baku-Tbilisi-Ceyhan (BTC) oil pipeline in Turkey experienced a rupture and fire in 2008. The Kurdish Workers Party claimed responsibility for the incident, but later investigations point to a cyber-attack in which the attackers accessed the control system of the pipeline via internet-connected security cameras and gained access to the industrial control systems to raise the pressure in the pipeline, causing it to rupture.

North-eastern blackout, USA and Canada, 2003
Malware may have inadvertently contributed to the 2003 blackout, which left 50 million North Americans without electricity. The blackout happened at a time when the computer worm Blaster affected a large number of computer systems, possibly impeding the timely detection of, and communication about, the initial small power outage, which cascaded to interconnected grids.

ANEXO II – DESTAQUES DAS REGULAMENTAÇÕES EUROPEIAS SOBRE A SEGURANÇA CIBERNÉTICA E PROTEÇÃO DE DADOS

DIRETIVA (UE) 2019/944 DO PARLAMENTO EUROPEU E DO CONSELHO
Funcionalidades dos sistemas de medidores inteligentes (Artigo 20) A segurança dos sistemas de medidores inteligentes e de comunicação de dados deve cumprir as regras da União Europeia aplicáveis em matéria de segurança, tendo em vista as melhores técnicas disponíveis, a fim de assegurar o mais elevado nível de proteção no campo da segurança cibernética, sem deixar de considerar os custos e o princípio da proporcionalidade. **Funções dos operadores de redes de transporte (Artigo 40)** Promover a gestão de dados, incluindo o desenvolvimento de sistemas de gestão de dados, a segurança cibernética e a proteção de dados, nos termos das disposições e regras aplicáveis, sem prejuízo daquelas de outras autoridades.

REGULAMENTO (UE) 2019/943 DO PARLAMENTO EUROPEU E DO CONSELHO
Funções da REORT para a Eletricidade (Artigo 30). Promover a segurança cibernética e a proteção de dados, em cooperação com as autoridades competentes e as entidades regulamentadas. **Funções da entidade ORDUE (Artigo 55)** Apoiar o desenvolvimento da gestão de dados, a segurança cibernética e a proteção de dados, em cooperação com as autoridades competentes e entidades regulamentadas. **Estabelecimento de códigos de rede (Artigo 59)** Regras setoriais para os aspetos ligados à segurança cibernética dos fluxos transfronteiriços de eletricidade, incluindo regras sobre os requisitos mínimos comuns, o planejamento, o acompanhamento e a elaboração de relatórios, assim como sobre a gestão de crises.

RECOMENDAÇÃO (UE) 2019/553 DA COMISSÃO
Requisitos em tempo real das componentes da infraestrutura energética Os Estados-Membros devem assegurar que os operadores de redes de energia, os fornecedores de tecnologias e, em especial, os operadores de serviços essenciais identificados na Diretiva SRI aplicam as medidas de preparação em matéria de segurança cibernética, relacionadas aos requisitos em tempo real no setor da energia.

Efeitos em cascata

Os Estados-Membros devem assegurar que os operadores de redes de energia, os fornecedores de tecnologias e, em especial, os operadores de serviços essenciais identificados na Diretiva SRI aplicam as medidas de preparação relacionadas aos efeitos em cascata no setor da energia. Considerando que as redes de eletricidade e os gasodutos estão fortemente interligados em toda a Europa, um ciberataque pode provocar uma falha ou perturbação que desencadeie efeitos em cascata de grande alcance a outros componentes.

Tecnologias antigas e de ponta

Os Estados-Membros devem assegurar que as partes interessadas, nomeadamente os operadores de redes de energia, os fornecedores de tecnologias e, em especial, os operadores de serviços essenciais identificados na Diretiva SRI, aplicam as medidas de preparação relacionadas à combinação de tecnologias clássicas e de ponta no setor da energia. Coexistem no sistema energético de hoje dois tipos diferentes de tecnologias: uma tecnologia mais antiga, com um tempo de vida de 30 a 60 anos, concebida antes de se utilizarem técnicas de segurança cibernética, e equipamentos modernos.

REGULAMENTO (UE) 2019/941 DO PARLAMENTO EUROPEU E DO CONSELHO

Autoridade competente (Artigo 3º)

Logo que possível e, em qualquer caso, até 5 de janeiro de 2020, cada Estado-Membro deve designar uma autoridade governamental ou um regulador nacional como autoridade competente, responsável pela execução das atribuições previstas no presente regulamento e que coopere com as autoridades dos outros Estados-Membros para efeitos dessa execução. Se for o caso, até que ocorra a designação, as entidades nacionais responsáveis pela segurança de abastecimento de eletricidade devem executar as atribuições da autoridade competente, nos termos do presente regulamento.

Avaliação dos riscos para a segurança de abastecimento de eletricidade (Artigo 4º)

Cada autoridade competente assegura que todos os riscos pertinentes relativos à segurança de abastecimento de eletricidade sejam avaliados de acordo com as normas do presente regulamento e do Capítulo IV do Regulamento (UE) 2019/943. Para tanto, a autoridade competente deve cooperar com os operadores das redes de transporte, os operadores das redes de distribuição, as entidades reguladoras, a REORT para a Eletricidade, os centros de coordenação regional e outras partes interessadas relevantes, conforme necessário.

Metodologia para identificar cenários de crise de eletricidade regionais (Artigo 5º)

Até 5 de janeiro de 2020, a REORT para a Eletricidade deve apresentar à ACER uma proposta de metodologia para identificar os cenários de crise de eletricidade regionais mais pertinentes.

A metodologia proposta deve identificar cenários de crise de eletricidade no que diz respeito à adequação e segurança do sistema e à segurança de aprovisionamento de combustível, com base, pelo menos, nos seguintes riscos:

a) Riscos naturais raros e extremos;
b) Riscos acidentais que excedam o critério de segurança N-1 e contingências excecionais; e
c) Riscos subsequentes, incluindo as consequências de ataques maliciosos e da escassez de combustível.

Adicionalmente, a metodologia proposta deve incluir, no mínimo, os seguintes elementos:

a) Consideração de todas as circunstâncias nacionais e regionais pertinentes, incluindo eventuais subgrupos;
b) Interação e correlação transfronteiriça de riscos;
c) Simulações de cenários de crises de eletricidade simultâneas;
d) Classificação dos riscos de acordo com o seu impacto e a sua probabilidade; e
e) Princípios que regem o tratamento de informações sensíveis, de forma a garantir a transparência perante o público.

Identificação de cenários de crise de eletricidade regionais (Artigo 6º)

No prazo de seis meses, a contar da aprovação de uma metodologia, nos termos do artigo 5º, nº 6, a REORT para a Eletricidade, com base nesta metodologia e em estreita cooperação com o GCE[20], os centros de coordenação regional, as autoridades competentes e as entidades reguladoras, deve identificar os cenários de crise de eletricidade mais pertinentes para cada região. A REORT para a Eletricidade pode delegar atribuições relacionadas à identificação dos cenários de crise de eletricidade regionais nos centros de coordenação regional.
A REORT para a Eletricidade deve apresentar os cenários de crise de eletricidade regionais aos operadores das redes de transporte pertinentes, aos centros de coordenação regional, às autoridades competentes e às entidades reguladoras, bem como ao GCE, podendo este recomendar alterações.

A REORT para a Eletricidade deve atualizar os cenários de crise de eletricidade regionais de quatro em quatro anos, salvo se as circunstâncias justificarem atualizações mais frequentes.

Identificação de cenários de crise de eletricidade nacionais (Artigo 7º)

[20] GCE - Grupo de Coordenação da Eletricidade, criado pela Decisão da Comissão de 15 de novembro de 2012.

No prazo de quatro meses, a contar da identificação dos cenários de crise de eletricidade regionais, nos termos do artigo 6º, nº 1, a autoridade competente deve identificar os cenários de crise de eletricidade nacionais mais pertinentes.

Ao identificar os cenários de crise de eletricidade nacionais, a autoridade competente deve consultar os operadores das redes de transporte, os operadores das redes de distribuição que considere relevantes, os produtores pertinentes ou as suas organizações setoriais e a entidade reguladora, caso esta não seja a autoridade competente.

Metodologia para avaliação da adequação sazonal e a curto prazo (Artigo 8º)

Até 5 de janeiro de 2020, a REORT para a Eletricidade deve apresentar à ACER uma proposta de metodologia para avaliar a adequação sazonal e de curto prazo, ou seja, a adequação mensal, para a semana seguinte ou, pelo menos, para o dia seguinte, que deve abranger, pelo menos, os seguintes aspetos:

a) Incerteza quanto a fatores como a probabilidade de um corte da capacidade de transporte, a probabilidade de uma interrupção imprevista de centrais elétricas, condições meteorológicas adversas, variabilidade da demanda, nomeadamente pontas de consumo associadas às condições meteorológicas, e variabilidade da geração de energia por fontes renováveis;
b) Probabilidade de ocorrência de uma crise de eletricidade; e
c) Probabilidade de ocorrência de crises de eletricidade simultâneas.

Elaboração de plano de preparação para riscos (Artigo 10)

Com base nos cenários de crise de eletricidade regionais e nacionais, identificados nos termos dos artigos 6º e 7º, a autoridade competente de cada Estado-Membro deve elaborar um plano de preparação para riscos, após consultar os operadores das redes de distribuição que considerar relevantes, os operadores das redes de transporte, os produtores pertinentes ou as suas organizações setoriais, as empresas de eletricidade e de gás natural, as organizações representem os interesses dos consumidores industriais e não industriais de eletricidade e a entidade reguladora, caso esta não seja a autoridade competente.

Conteúdo dos planos de preparação para riscos com medidas regionais e bilaterais (Artigo 12)

Além das medidas nacionais a que se refere o artigo 11, o plano de preparação para riscos de cada Estado--Membro deve incluir medidas regionais e, se for o caso, bilaterais, destinadas a assegurar que as crises de eletricidade com impacto transfronteiriço sejam devidamente prevenidas e geridas. As medidas regionais devem ser acordadas na região em questão, entre os Estados-Membros com capacidade técnica para prestar assistência mútua, nos termos do artigo 15. Para tanto, os Estados-Membros podem igualmente criar subgrupos dentro de uma região. As medidas bilaterais devem ser acordadas entre os Estados-Membros que estão diretamente ligados, mas

que não fazem parte da mesma região. Os Estados-Membros devem assegurar a coerência entre as medidas regionais e bilaterais.

Avaliação dos planos de preparação para riscos pela Comissão Europeia (Artigo 13)

No prazo de quatro meses, a contar da notificação do plano de preparação para riscos adotado pela autoridade competente, a Comissão Europeia deve avalia-lo, considerando os pontos expressos pelo GCE.

Após consultar o GCE, a Comissão Europeia deverá emitir um parecer não vinculativo, devidamente fundamentado, e apresentá-lo à autoridade competente.

Alerta precoce e declaração de crise de eletricidade (Artigo 14)

Sempre que uma avaliação da adequação sazonal ou outra fonte qualificada contiver informações concretas, sérias e confiáveis de que pode ocorrer uma crise de eletricidade em um Estado-Membro, a autoridade competente deste Estado-Membro deve emitir, sem demora indevida, um alerta à Comissão Europeia, às autoridades competentes dos Estados--Membros da mesma região e, caso não façam parte da mesma região, às autoridades competentes dos Estados-Membros diretamente ligados.

A autoridade competente em questão deve também fornecer informações sobre as causas da possível crise de eletricidade, as medidas tomadas ou previstas para prevenir uma crise de eletricidade e a eventual necessidade de assistência por parte de outros Estados-Membros. As informações devem incluir, ainda, o eventual impacto das medidas no mercado interno da eletricidade. A Comissão Europeia deverá transmitir essas informações ao GCE.

Quando confrontada com uma crise de eletricidade, a autoridade competente, após consultar o operador da rede de transporte em questão, deve declarar a crise e informar, sem demora indevida, as autoridades competentes dos Estados-Membros da mesma região e, caso não façam parte da mesma região, as autoridades competentes dos Estados-Membros diretamente ligados e a Comissão Europeia. Essas informações devem incluir as causas da deterioração da situação de fornecimento de eletricidade, as razões que levaram a declarar uma crise de eletricidade, as medidas tomadas ou previstas para atenuá-la e a eventual necessidade de assistência por parte de outros Estados-Membros.

Cooperação e assistência (Artigo 15)

Os Estados-Membros devem atuar e cooperar com um espírito de solidariedade na prevenção e gestão de crises de eletricidade.

Caso disponham da capacidade técnica necessária, os Estados-Membros devem oferecer assistência mútua por meio de medidas regionais ou bilaterais, que tenham sido acordadas nos termos do presente artigo e do artigo 12, antes que a assistência seja prestada.

Para o efeito e no intuito de preservar a segurança pública e das pessoas, os Estados-Membros devem firmar um acordo sobre as disposições técnicas, jurídicas e financeiras necessárias para a execução das medidas regionais ou bilaterais, antes de oferecerem a assistência. Estas disposições devem especificar, nomeadamente, a quantidade máxima de eletricidade a fornecer a nível regional ou bilateral, o fator de desencadeamento de qualquer assistência e da sua suspensão, a forma como a eletricidade será fornecida e as questões em matéria de compensação justa entre Estados-Membros, nos termos dos artigos 4º, 5º e 6º.

Observância das regras de mercado (Artigo 16)

As medidas tomadas para prevenir ou atenuar crises de eletricidade devem respeitar as regras que regulam o mercado interno de eletricidade e a operação da rede.

Em uma situação de crise de eletricidade, as medidas não baseadas no mercado somente serão aplicadas em último recurso, caso tenham sido esgotadas todas as opções facultadas pelo mercado ou caso seja evidente que as medidas baseadas no mercado não são, por si só, suficientes para evitar que a situação de fornecimento de eletricidade se deteriore.

As medidas não baseadas no mercado não podem abalar indevidamente a concorrência nem o funcionamento eficaz do mercado da eletricidade, devendo ser necessárias, proporcionais, não discriminatórias e temporárias.

A autoridade competente deve informar as partes interessadas relevantes do seu Estado-Membro sobre a aplicação de quaisquer medidas não baseadas no mercado.

Avaliação *ex post* (Artigo 17)

Logo que possível ou, em qualquer caso, até três meses após o fim de uma crise de eletricidade, a autoridade competente do Estado-Membro que declarou a crise deve apresentar um relatório de avaliação *ex post* ao GCE e à Comissão Europeia, depois de consultar a entidade reguladora, caso esta não seja a autoridade competente.

Acompanhamento (Artigo 18)

Além de executar outras atribuições previstas no presente regulamento, o GCE deve debater:

a) O plano decenal de desenvolvimento da rede de eletricidade, elaborado pela REORT para a Eletricidade; e

b) A coerência dos planos de preparação para riscos, adotados pelas autoridades competentes.

Tratamento de informações confidenciais (Artigo 19)

Os Estados-Membros e as autoridades competentes devem aplicar os procedimentos referidos no presente regulamento em conformidade com as regras aplicáveis, designadamente as regras nacionais relativas ao tratamento de informações e processos confidenciais. Se a aplicação de tais regras tiver como consequência a não divulgação de determinadas informações, nomeadamente no âmbito dos planos de preparação para riscos, o Estado-Membro ou a autoridade competente pode, mediante pedido neste sentido, fornecer uma síntese não confidencial das mesmas.

A Comissão, a ACER, o GCE, a REORT para a Eletricidade, os Estados-Membros, as autoridades competentes, as entidades reguladoras e quaisquer outros organismos, entidades ou pessoas pertinentes, que recebam informações confidenciais ao abrigo do presente regulamento, devem assegurar a confidencialidade das informações sensíveis.

ANEXO III – LISTA DE SIGLAS E ACRÔNIMOS

Term	Definition
AMI	Advanced Metering Infrastructure
ANSSI	French Network and Information Security Agency
BATs	Best Available Technics
BREF	Best Available Technics reference document
CAPEX	Capital expenditure
CEER	Council of European Energy Regulators
CERT	Computer Emergency Response Team
CS WS	Cybersecurity Work Stream
CSIRT	Computer Security Incident Response Team
DG Energy	Directorate-General for Energy
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
DSO	Distribution System Operator
EC SG TF EG	European Commission Smart Grids Task Force Expert Group
EEA	European Economic Area
EECSP	European Energy Cyber Security Platform
EFTA	European Free Trade Association
ENISA	European Union Agency for Network and Information Security
EU	European Union
Europol	European Union Agency for Law Enforcement Cooperation
Exploit	Software of set of commands taking advantage of a bug or vulnerability to cause unintended behaviour
GDPR	General Data Protection Regulation
GGP	Guidelines of Good Practice
Hack	To break into computers and computer networks
ICT	Information and Communications Technology
ID number	Identity number
IoT	Internet of Things
Malware	Hostile or intrusive software
MO	Metering Operator
MS	Member State (of the European Union)
Nation-state	Political entity on a territory coinciding with its citizens
NISD	Directive concerning measures for a high common level of security of Network and Information Systems across the Union
NRA	National Regulatory Authority
OES	Operators of Essential Services
OPEX	Operational expenditure

Term	Definition
REMIT	Regulation (EU) No 1227/2011 of the European Parliament and of the Council on wholesale energy market integrity and transparency
SCADA	Supervisory Control and Data Acquisition
SGO	Smart Grid Operator
SO	System Operator
Trojan	Malicious computer program misleading users of its true intent
TSO	Transmission System Operator
Wiper	Malware with the aim to wipe the hard drive of the computer it infects
Worm	Malicious computer program that replicates itself to spread to other computers

Grupo de Estudos do Setor elétrico
Gesel

Toda a produção acadêmica e científica do GESEL está disponível no site do Grupo, que também mantém uma intensa relação com o setor através das redes sociais Facebook e Twitter.

Destaca-se ainda a publicação diária do IFE - Informativo Eletrônico do Setor Elétrico, editado deste 1998 e distribuído para mais de 10.000 usuários, onde são apresentados resumos das principais informações, estudos e dados sobre o setor elétrico do Brasil e exterior, podendo ser feita inscrição gratuita em http://cadastro-ife.gesel.ie.ufrj.br

GESEL – Destacado think tank do setor elétrico brasileiro, fundado em 1997, desenvolve estudos buscando contribuir com o aperfeiçoamento do modelo de estruturação e funcionamento do Setor Elétrico Brasileiro (SEB). Além das pesquisas, artigos acadêmicos, relatórios técnicos e livros – em grande parte associados a projetos realizados no âmbito do Programa de P&D da Aneel – ministra cursos de qualificação para as instituições e agentes do setor e realiza eventos – work shops, seminários, visitas e reuniões técnicas – no Brasil e no exterior. Ao nível acadêmico é responsável pela área de energia elétrica do Programa de Pós-Graduação em Políticas Públicas, Estratégias e Desenvolvimento do Instituto de Economia (PPED) do Instituto de Economia da UFRJ

ISBN: 978-65-86614-23-7

SITE: gesel.ie.ufrj.br

FACEBOOK: facebook.com/geselufrj

TWITTER: twitter.com/geselufrj

E-MAIL: gesel@gesel.ie.ufrj.br

TELEFONE: (21) 3938-5249
(21) 3577-3953

Scan me

Versão Digital

ENDEREÇO:

UFRJ - Instituto de Economia.
Campus da Praia Vermelha.

Av. Pasteur 250, sala 226 - Urca.
Rio de Janeiro, RJ - Brasil.
CEP: 22290-240