



2024/1366

24.5.2024

REGULAMENTO DELEGADO (UE) 2024/1366 DA COMISSÃO

de 11 de março de 2024

que completa o Regulamento (UE) 2019/943 do Parlamento Europeu e do Conselho estabelecendo um código de rede relativo a regras setoriais para os aspetos ligados à cibersegurança dos fluxos transfronteiriços de eletricidade

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) 2019/943 do Parlamento Europeu e do Conselho, de 5 de junho de 2019, relativo ao mercado interno da eletricidade ⁽¹⁾, nomeadamente o artigo 59.º, n.º 2, alínea e),

Considerando o seguinte:

- (1) A gestão dos riscos de cibersegurança é crucial para manter a segurança do abastecimento de eletricidade e para assegurar um nível elevado de cibersegurança no setor da eletricidade.
- (2) A digitalização e a cibersegurança são decisivas para a prestação de serviços essenciais e, por conseguinte, de importância estratégica para as infraestruturas energéticas críticas.
- (3) A Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho ⁽²⁾ estabelece medidas destinadas a garantir um elevado nível comum de cibersegurança na União. O Regulamento (UE) 2019/941 do Parlamento Europeu e do Conselho ⁽³⁾ complementa a Diretiva (UE) 2022/2555, assegurando que os incidentes de cibersegurança no setor da eletricidade são devidamente identificados como um risco e que as medidas tomadas para os resolver são devidamente abordadas nos planos de preparação para riscos. O Regulamento (UE) 2019/943 complementa a Diretiva (UE) 2022/2555 e o Regulamento (UE) 2019/941, estabelecendo regras específicas para o setor da eletricidade a nível da União. Além disso, o presente regulamento delegado complementa as disposições da Diretiva (UE) 2022/2555 relativas ao setor da eletricidade, sempre que estejam em causa fluxos transfronteiriços de eletricidade.
- (4) Num contexto de redes de eletricidade digitalizadas interligadas, a prevenção e a gestão de crises de eletricidade relacionadas com ciberataques não podem ser consideradas uma tarefa exclusivamente nacional. Importa elaborar medidas mais eficientes e menos onerosas por meio da cooperação regional e a nível da União, de forma a explorar todo o seu potencial. Por conseguinte, é necessário um quadro comum de regras e procedimentos mais bem coordenados, a fim de assegurar que os Estados-Membros e outros intervenientes possam cooperar eficazmente além-fronteiras, num espírito de maior transparência, confiança e solidariedade entre os Estados-Membros e as autoridades competentes responsáveis pela eletricidade e pela cibersegurança.
- (5) A gestão dos riscos de cibersegurança no âmbito do presente regulamento exige um processo estruturado que inclua, nomeadamente, a identificação dos riscos para os fluxos transfronteiriços de eletricidade decorrentes de ciberataques, os processos operacionais e perímetros conexos, bem como os controlos e mecanismos de verificação da cibersegurança correspondentes. Embora o calendário para todo o processo esteja repartido por vários anos, cada etapa deve contribuir para um elevado nível comum de cibersegurança no setor e para a atenuação dos riscos de cibersegurança. Todos os participantes no processo devem esforçar-se ao máximo para criar e chegar a acordo sobre as metodologias o mais rapidamente possível, sem demora injustificada e, em qualquer caso, o mais tardar nos prazos definidos no presente regulamento.

⁽¹⁾ JO L 158 de 14.6.2019, p. 54.

⁽²⁾ Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2) (JO L 333 de 27.12.2022, p. 80).

⁽³⁾ Regulamento (UE) 2019/941 do Parlamento Europeu e do Conselho, de 5 de junho de 2019, relativo à preparação para riscos no setor da eletricidade e que revoga a Diretiva 2005/89/CE (JO L 158 de 14.6.2019, p. 1).

- (6) As avaliações dos riscos de cibersegurança à escala da União, a nível regional, do Estado-Membro, e da entidade previstas no presente regulamento podem limitar-se às resultantes de ciberataques, na aceção do Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho ⁽⁴⁾, excluindo, por conseguinte, por exemplo, ataques físicos, catástrofes naturais e indisponibilidades devido à perda de instalações ou de recursos humanos. Os riscos à escala da União e a nível regional relacionados com ataques físicos ou catástrofes naturais no domínio da eletricidade já estão abrangidos por outra legislação da União em vigor, nomeadamente o artigo 5.º do Regulamento (UE) 2019/941 ou o Regulamento (UE) 2017/1485 da Comissão ⁽⁵⁾, que estabelece orientações para a operação de redes de transporte de eletricidade. Do mesmo modo, a Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho ⁽⁶⁾, relativa à resiliência das entidades críticas visa reduzir as vulnerabilidades e reforçar a resiliência física das entidades críticas e abrange todos os riscos naturais e de origem humana pertinentes que possam afetar a prestação de serviços essenciais, nomeadamente acidentes, catástrofes naturais, emergências de saúde pública como as pandemias e as ameaças híbridas ou outras ameaças antagonistas, incluindo infrações terroristas, infiltrações criminosas e sabotagens.
- (7) A noção de «entidades de impacto elevado e de impacto crítico» no presente regulamento é fundamental para definir o âmbito das entidades que estarão sujeitas às obrigações descritas no presente regulamento. A abordagem baseada no risco descrita nas diferentes disposições visa identificar os processos, os ativos de apoio e as entidades que os exploram que afetam os fluxos transfronteiriços de eletricidade. Dependendo do grau de impacto de eventuais ciberataques nas suas operações de fluxos transfronteiriços de eletricidade, estas podem ser consideradas de «impacto elevado» ou de «impacto crítico». O artigo 3.º da Diretiva (UE) 2022/2555 estabelece as noções de entidades essenciais e entidades importantes e os critérios para identificar as entidades com essas categorias. Embora muitas delas sejam consideradas e identificadas simultaneamente como «essenciais» na aceção do artigo 3.º da Diretiva (UE) 2022/2555 e de impacto elevado ou de impacto crítico nos termos do artigo 24.º do presente regulamento, os critérios estabelecidos neste último referem-se unicamente ao papel e impacto das entidades nos processos de eletricidade que afetam os fluxos transfronteiriços, sem ter em conta os critérios definidos no artigo 3.º da Diretiva (UE) 2022/2555.
- (8) As entidades abrangidas pelo âmbito de aplicação do presente regulamento, consideradas de impacto elevado ou de impacto crítico nos termos do artigo 24.º do presente regulamento e sujeitas às obrigações nele estabelecidas, são principalmente as que têm um impacto direto nos fluxos transfronteiriços de eletricidade na UE.
- (9) Para garantir a eficiência e evitar duplicações na consecução dos objetivos, o presente regulamento recorre aos mecanismos e instrumentos já estabelecidos noutras legislações.
- (10) Ao aplicarem o presente regulamento, os Estados-Membros, as autoridades competentes e os operadores das redes devem ter em conta as normas europeias acordadas e as especificações técnicas das organizações europeias de normalização e agir em conformidade com a legislação da União relativa à colocação no mercado ou à colocação em serviço de produtos abrangidos por essa legislação da União.

⁽⁴⁾ Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 (JO L 333 de 27.12.2022, p. 1).

⁽⁵⁾ Regulamento (UE) 2017/1485 da Comissão, de 2 de agosto de 2017, que estabelece orientações sobre a operação de redes de transporte de eletricidade (JO L 220 de 25.8.2017, p. 1).

⁽⁶⁾ Regulamento (UE) 2022/2557 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa à resiliência das entidades críticas e que revoga a Diretiva 2008/114/CE do Conselho (JO L 333 de 27.12.2022, p. 164).

- (11) Com vista a atenuar os riscos de cibersegurança, é necessário criar um manual de regras pormenorizado para reger as ações e a cooperação entre as partes interessadas cujas atividades digam respeito a aspetos de cibersegurança dos fluxos transfronteiriços de eletricidade, com o objetivo de garantir a segurança da rede. Essas regras organizacionais e técnicas devem assegurar que a maioria dos incidentes de eletricidade com causas profundas a nível de cibersegurança é eficazmente tratada a nível operacional. É necessário definir o que essas partes interessadas devem fazer para evitar tais crises e as medidas que podem tomar se as regras de exploração da rede já não forem, por si só, suficientes. Por conseguinte, é necessário criar um regime comum de regras sobre a prevenção das crises de eletricidade simultâneas cujas causas profundas tenham a ver com a cibersegurança, a preparação para essas crises e a gestão das mesmas. Deste modo, aumenta-se a transparência na fase de preparação e durante uma crise simultânea de eletricidade, assegurando-se que as medidas são tomadas de forma coordenada e eficaz em conjunto com as autoridades competentes em matéria de cibersegurança nos Estados-Membros. Os Estados-Membros e as entidades pertinentes devem ser obrigados a cooperar a nível regional e, se for caso disso, a nível bilateral, num espírito de solidariedade. Essa cooperação e as regras destinam-se a obter uma melhor preparação para riscos de cibersegurança a custos mais baixos, também em consonância com os objetivos da Diretiva (UE) 2022/2555. Afigura-se igualmente necessário reforçar o mercado interno da eletricidade fomentando a confiança entre Estados-Membros, em especial atenuando o risco de restrição indevida dos fluxos transfronteiriços de eletricidade, reduzindo assim o risco de efeitos colaterais negativos nos Estados-Membros vizinhos.
- (12) A segurança do abastecimento de eletricidade implica uma cooperação eficaz entre os Estados-Membros, as instituições, os órgãos e os organismos da União e as partes interessadas relevantes. Os operadores das redes de distribuição e os operadores das redes de transporte desempenham um papel fundamental na garantia de uma rede de eletricidade segura, fiável e eficiente, em conformidade com os artigos 31.º e 40.º da Diretiva (UE) 2019/944 do Parlamento Europeu e do Conselho ⁽⁷⁾. As várias entidades reguladoras e outras autoridades nacionais competentes também desempenham um papel importante na garantia e no controlo da cibersegurança no abastecimento de eletricidade, no âmbito das respetivas funções previstas nas Diretivas (UE) 2019/944 e (UE) 2022/2555. Os Estados-Membros devem designar uma entidade existente ou nova como sua autoridade nacional competente para a aplicação do presente regulamento, com o objetivo de assegurar a participação transparente e inclusiva de todos os intervenientes, a preparação eficiente e correta aplicação do dito regulamento, a cooperação entre as diferentes partes interessadas pertinentes e as autoridades competentes nos domínios da eletricidade e da cibersegurança, bem como facilitar a prevenção e a avaliação *ex post* de crises de eletricidade com causas profundas a nível de cibersegurança e o intercâmbio de informações sobre as mesmas.
- (13) Se uma entidade de impacto elevado ou de impacto crítico prestar serviços em mais do que um Estado-Membro, ou tiver a sua sede, outro estabelecimento ou um representante num Estado-Membro mas os seus sistemas de rede e informação estiverem situados noutra ou noutros Estados-Membros, esses Estados-Membros devem incentivar as respetivas autoridades competentes a envidar todos os esforços para cooperar entre si e prestar assistência mútua, na medida do necessário.
- (14) Os Estados-Membros devem assegurar que as autoridades competentes dispõem dos poderes necessários em relação às entidades de impacto elevado e de impacto crítico para promover o cumprimento do presente regulamento. Esses poderes devem possibilitar que as autoridades competentes realizem inspeções no local e supervisão fora do local, o que pode incluir controlos aleatórios, a realização de auditorias periódicas, auditorias de segurança específicas com base em avaliações de risco ou informações disponíveis relacionadas com os riscos, bem como verificações de segurança com base em critérios de avaliação dos riscos objetivos, não discriminatórios, equitativos e transparentes e que incluam o pedido das informações necessárias para avaliar as medidas de cibersegurança adotadas pela entidade. Essas informações devem incluir políticas de cibersegurança documentadas, dados de acesso, documentos ou quaisquer informações necessárias para o desempenho das suas funções de supervisão, bem como provas da aplicação das políticas de cibersegurança, como os resultados de auditorias de segurança efetuadas por um auditor qualificado e os respetivos elementos de prova subjacentes.

⁽⁷⁾ Diretiva (UE) 2019/944 do Parlamento Europeu e do Conselho, de 5 de junho de 2019, relativa a regras comuns para o mercado interno da eletricidade e que altera a Diretiva 2012/27/UE (JO L 158 de 14.6.2019, p. 125).

- (15) A fim de evitar lacunas ou duplicações das obrigações de gestão dos riscos de cibersegurança impostas a entidades de impacto elevado e de impacto crítico, as autoridades nacionais nos termos da Diretiva (UE) 2022/2555 e as autoridades competentes nos termos do presente regulamento devem cooperar no que respeita à aplicação de medidas de gestão dos riscos de cibersegurança e à supervisão do cumprimento dessas medidas a nível nacional. As autoridades competentes nos termos da Diretiva (UE) 2022/2555 podem considerar que uma entidade que cumpre os requisitos de gestão dos riscos de cibersegurança estabelecidos no presente regulamento garante o cumprimento dos requisitos correspondentes estabelecidos nessa diretiva, ou vice-versa.
- (16) Uma abordagem comum para a prevenção e gestão de crises de eletricidade simultâneas exige um entendimento comum entre os Estados-Membros sobre o que constitui uma crise de eletricidade simultânea e quando um ciberataque é um fator importante. Em especial, deverá ser facilitada a coordenação entre os Estados-Membros e as entidades pertinentes para fazer face a uma situação na qual o risco potencial de escassez significativa de eletricidade ou de impossibilidade de fornecer eletricidade aos clientes esteja presente ou iminente devido a um ciberataque.
- (17) O considerando 1 do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho⁽⁸⁾ reconhece o papel crucial das redes e dos sistemas de informação e das redes e dos serviços de comunicações eletrónicas para assegurar o funcionamento da economia em setores determinantes como a energia, enquanto o considerando 44 explica que a Agência da União Europeia para a Cibersegurança (ENISA) deve estabelecer ligações com a Agência da União Europeia de Cooperação dos Reguladores da Energia (ACER).
- (18) O Regulamento (UE) 2019/943 atribui responsabilidades específicas em matéria de cibersegurança aos operadores das redes de transporte (ORT) e aos operadores das redes de distribuição (ORD). As suas associações europeias, nomeadamente a rede europeia de ORT de eletricidade («REORT para a Eletricidade») e a entidade europeia para os ORD («entidade ORDUE»), devem, nos termos dos artigos 30.º e 55.º do referido regulamento, respetivamente, promover a cibersegurança em cooperação com as autoridades competentes e as entidades regulamentadas.
- (19) Uma abordagem comum da prevenção e gestão de crises de eletricidade simultâneas com causas profundas a nível de cibersegurança exige igualmente que todas as partes interessadas pertinentes utilizem métodos e definições harmonizados para identificar os riscos relacionados com a cibersegurança do abastecimento de eletricidade. Exige também que estejam em condições de comparar eficazmente o seu desempenho e o dos seus vizinhos nesse domínio. Por conseguinte, é necessário estabelecer os processos e as funções e responsabilidades para elaborar e atualizar metodologias de gestão de riscos, escalas de classificação de incidentes e medidas de cibersegurança adaptadas aos riscos de cibersegurança que afetam os fluxos transfronteiriços de eletricidade.
- (20) Os Estados-Membros, por intermédio da autoridade competente designada para efeitos do presente regulamento, são responsáveis pela identificação das entidades que cumprem os critérios para serem consideradas entidades de impacto elevado e de impacto crítico. A fim de eliminar as divergências entre os Estados-Membros nesse domínio e proporcionar a todas as entidades pertinentes segurança jurídica no que respeita às medidas de gestão de riscos de cibersegurança e às obrigações de elaboração de relatórios, há que estabelecer um conjunto de critérios para identificar as entidades abrangidas pelo presente regulamento. Esse conjunto de critérios deve ser definido e periodicamente atualizado no âmbito do processo de elaboração e adoção de termos, condições e metodologias estabelecidos no presente regulamento.
- (21) As disposições do presente regulamento deverão aplicar-se sem prejuízo do direito da União que preveja regras específicas em matéria de certificação de produtos, serviços e processos de tecnologias de informação e comunicação (TIC), em especial o Regulamento (UE) 2019/881 no que respeita ao quadro para a criação de sistemas europeus de certificação da cibersegurança. No contexto do presente regulamento, os produtos de TIC deverão também incluir dispositivos técnicos e programas informáticos que possibilitem a interação direta com a rede eletrotécnica, em especial sistemas de controlo industrial que possam ser utilizados para o transporte, a distribuição e a produção de energia, bem como para a recolha e transmissão de informações conexas. As disposições devem assegurar que os produtos, serviços e processos de TIC a adquirir cumprem os objetivos de segurança pertinentes previstos no artigo 51.º do Regulamento (UE) 2019/881.

⁽⁸⁾ Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança) (JO L 151 de 7.6.2019, p. 15).

- (22) Os ciberataques recentes mostram que as entidades estão a tornar-se cada vez mais alvo de ataques à cadeia de abastecimento que, além de terem impacto nas entidades individuais abrangidas, também podem ter um efeito em cascata em ataques de maior dimensão contra entidades às quais estão ligadas na rede de eletricidade. Por conseguinte, foram acrescentadas disposições e recomendações para ajudar a atenuar os riscos de cibersegurança associados aos processos relacionados com a cadeia de abastecimento, nomeadamente a contratação, com impacto nos fluxos transfronteiriços de eletricidade.
- (23) Uma vez que a exploração de vulnerabilidades dos sistemas de rede e informação pode causar perturbações e danos energéticos consideráveis à economia e aos consumidores, essas vulnerabilidades devem ser rapidamente identificadas e corrigidas, para reduzir os riscos. A fim de facilitar a aplicação efetiva do presente regulamento, as entidades pertinentes e as autoridades competentes devem cooperar no sentido de exercer e testar atividades consideradas adequadas para o efeito, incluindo o intercâmbio de informações sobre ciberameaças, ciberataques, vulnerabilidades, ferramentas e métodos, táticas, técnicas e procedimentos, preparação para a gestão de crises de cibersegurança e outros exercícios. Uma vez que a tecnologia está em constante evolução e a digitalização do setor da eletricidade está a avançar rapidamente, a aplicação das disposições adotadas não deve prejudicar a inovação nem constituir um obstáculo ao acesso ao mercado da eletricidade e à subsequente utilização de soluções inovadoras que contribuam para a eficiência e a sustentabilidade da rede de eletricidade.
- (24) As informações recolhidas com vista ao acompanhamento da aplicação do presente regulamento devem ser razoavelmente limitadas com base no princípio da necessidade de conhecer. Importa conceder às partes interessadas prazos exequíveis e eficazes para a apresentação dessas informações, devendo evitar-se a dupla notificação.
- (25) A proteção da cibersegurança não termina nas fronteiras da União. Uma rede segura exige a participação de países terceiros vizinhos. A União e os seus Estados-Membros devem esforçar-se por apoiar os países terceiros vizinhos, cuja infraestrutura de eletricidade esteja ligada à rede europeia, na aplicação de regras de cibersegurança semelhantes às estabelecidas no presente regulamento.
- (26) A fim de melhorar a coordenação da segurança numa fase precoce e testar futuros termos, condições e metodologias vinculativos, a REORT para a Eletricidade, a entidade ORDUE e as autoridades competentes devem começar a elaborar orientações não vinculativas imediatamente após a entrada em vigor do presente regulamento. Essas orientações servirão de base para o desenvolvimento dos futuros termos, condições e metodologias. Paralelamente, as autoridades competentes devem identificar as entidades candidatas a entidades de impacto elevado e de impacto crítico para começarem voluntariamente a cumprir as obrigações.
- (27) O presente regulamento foi elaborado em estreita cooperação com a ACER, a ENISA, a REORT para a Eletricidade, a entidade ORDUE e outras partes interessadas, com vista à adoção transparente e participativa de regras eficazes, equilibradas e proporcionadas.
- (28) O presente regulamento complementa e reforça as medidas de gestão de crises estabelecidas no quadro de resposta da UE a crises de cibersegurança, tal como estabelecido na Recomendação (UE) 2017/1584 da Comissão⁽⁹⁾. Um ciberataque pode também causar, contribuir ou coincidir com uma crise de eletricidade, na aceção do artigo 2.º, ponto 9), do Regulamento (UE) 2019/941, com impacto nos fluxos transfronteiriços de eletricidade. Essa crise de eletricidade pode conduzir a uma crise de eletricidade simultânea, na aceção do artigo 2.º, ponto 10), do Regulamento (UE) 2019/941, podendo esse incidente ter também impacto noutros setores dependentes da segurança do abastecimento de eletricidade. Se o incidente se agravar para um incidente de cibersegurança em grande escala na aceção do artigo 16.º da Diretiva (UE) 2022/2555, devem aplicar-se as disposições desse artigo que cria a Rede Europeia de Organizações de Coordenação de Cibercrises (UE-CyCLONe). No atinente à gestão de crises a nível da União, as partes responsáveis deverão recorrer ao Mecanismo Integrado da UE de Resposta Política a Situações de Crise («mecanismo IPCR») previsto na Decisão de Execução (UE) 2018/1993 do Conselho⁽¹⁰⁾.
- (29) O presente regulamento não prejudica a competência dos Estados-Membros para tomarem as medidas necessárias a fim de garantir a proteção dos interesses essenciais da sua própria segurança, salvaguardar a ordem e a segurança pública e permitir a investigação, a deteção e a repressão de infrações penais, em conformidade com o direito da União. Nos termos do artigo 346.º do TFUE, nenhum Estado-Membro é obrigado a fornecer informações cuja divulgação considere contrária aos interesses essenciais da sua própria segurança.

⁽⁹⁾ Recomendação (UE) 2017/1584 da Comissão, de 13 de setembro de 2017, sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala (JO L 239 de 19.9.2017, p. 36).

⁽¹⁰⁾ Decisão de Execução (UE) 2018/1993 do Conselho, de 11 de dezembro de 2018, relativa ao Mecanismo Integrado da UE de Resposta Política a Situações de Crise (JO L 320 de 17.12.2018, p. 28).

- (30) Embora o presente regulamento se aplique, em princípio, a entidades que exercem atividades de produção de eletricidade a partir de centrais nucleares, algumas dessas atividades podem estar ligadas à segurança nacional.
- (31) O direito da União em matéria de proteção de dados e o direito da União em matéria de privacidade devem ser aplicáveis a qualquer tratamento de dados pessoais realizado ao abrigo do presente regulamento. Em especial, o presente regulamento não prejudica o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ⁽¹⁾, a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho ⁽²⁾ e o Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ⁽³⁾. Por conseguinte, o presente regulamento não deverá afetar, nomeadamente, as funções e os poderes das autoridades competentes para acompanhar o cumprimento do direito da União em matéria de proteção de dados e do direito da União em matéria de privacidade aplicáveis.
- (32) Dada a importância da cooperação internacional em matéria de cibersegurança, as autoridades competentes responsáveis pelo exercício das funções atribuídas pelo presente regulamento e designadas pelos Estados-Membros deverão poder participar nas redes de cooperação internacional. Por conseguinte, para efeitos do exercício das suas funções, as autoridades competentes deverão poder trocar informações, incluindo dados pessoais, com as autoridades competentes de países terceiros, desde que sejam cumpridas as condições previstas no direito da União em matéria de proteção de dados para as transferências de dados pessoais para países terceiros, nomeadamente no artigo 49.º do Regulamento (UE) 2016/679.
- (33) O tratamento de dados pessoais, efetuado na medida estritamente necessária e proporcionada para assegurar a segurança dos ativos por entidades de impacto elevado ou de impacto crítico, poderá ser considerado lícito pelo facto de respeitar uma obrigação jurídica a que o responsável pelo tratamento está sujeito, em conformidade com os requisitos estabelecidos pelo artigo 6.º, n.º 1, alínea c), e pelo artigo 6.º, n.º 3, do Regulamento (UE) 2016/679. O tratamento de dados pessoais pode também ser necessário para efeito dos interesses legítimos prosseguidos por entidades de impacto elevado ou de impacto crítico, bem como por fornecedores de tecnologias e prestadores de serviços de segurança que atuem em nome dessas entidades, nos termos do artigo 6.º, n.º 1, alínea f), do Regulamento (UE) 2016/679, nomeadamente quando tal tratamento é necessário aos acordos de partilha de informações sobre cibersegurança ou à notificação voluntária de informações pertinentes em conformidade com o presente regulamento. Medidas relacionadas com a prevenção, deteção, identificação, contenção, análise e resposta a ciberataques, medidas de sensibilização relativas a ciberameaças específicas, intercâmbio de informações no contexto da correção e da divulgação coordenada de vulnerabilidades, bem como o intercâmbio voluntário de informações sobre esses ciberataques, ciberameaças e vulnerabilidades, indicadores de exposição a riscos, táticas, técnicas e procedimentos, alertas de cibersegurança e ferramentas de configuração podem implicar o tratamento de determinadas categorias de dados pessoais, tais como endereços IP, localizadores uniformes de recursos (URL), nomes de domínio, endereços de correio eletrónico e, sempre que revelem dados pessoais, selos temporais. O tratamento de dados pessoais pelas autoridades competentes, pelos pontos de contacto únicos e pelas CSIRT pode constituir uma obrigação jurídica ou ser considerado necessário para o exercício de uma missão de interesse público ou da autoridade pública de que está investido o responsável pelo tratamento, nos termos do artigo 6.º, n.º 1, alíneas c) ou e), e do artigo 6.º, n.º 3, do Regulamento (UE) 2016/679, ou para a prossecução de um interesse legítimo das entidades de impacto elevado ou de impacto crítico, tal como referido no artigo 6.º, n.º 1, alínea f), do referido regulamento. Além disso, o direito nacional pode estabelecer regras que, na medida do necessário e proporcionado para garantir a segurança dos sistemas de rede e informação de entidades de impacto elevado e de impacto crítico, permitam às autoridades competentes, aos balcões únicos e às CSIRT tratar categorias especiais de dados pessoais em conformidade com o artigo 9.º do Regulamento (UE) 2016/679, mormente prevendo medidas adequadas e específicas para salvaguardar os direitos e interesses fundamentais das pessoas singulares, nomeadamente restrições técnicas no que respeita à reutilização desses dados e o recurso às medidas tecnologicamente mais avançadas em matéria de segurança e de preservação da privacidade, como a pseudonimização ou a cifragem, sempre que a anonimização possa afetar significativamente a finalidade prosseguida.

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

⁽²⁾ Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37).

⁽³⁾ Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).

- (34) Os dados pessoais ficam amiúde comprometidos em consequência de ciberataques. Nesse contexto, as entidades competentes deverão cooperar e trocar informações sobre todas as questões pertinentes com as autoridades referidas no Regulamento (UE) 2016/679 e na Diretiva 2002/58/CE.
- (35) A Autoridade Europeia para a Proteção de Dados foi consultada em conformidade com o artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 e emitiu parecer em 17 de novembro de 2023,

ADOTOU O PRESENTE REGULAMENTO:

Capítulo I

DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto

O presente regulamento cria um código de rede que estabelece regras setoriais para os aspetos ligados à cibersegurança dos fluxos transfronteiriços de eletricidade, incluindo regras sobre os requisitos mínimos comuns, o planeamento, o acompanhamento, a elaboração de relatórios e a gestão de crises.

Artigo 2.º

Âmbito de aplicação

1. O presente regulamento aplica-se aos aspetos ligados à cibersegurança dos fluxos transfronteiriços de eletricidade nas atividades das seguintes entidades, se forem identificadas como entidades de impacto elevado ou de impacto crítico em conformidade com o artigo 24.º:

- a) Empresas de eletricidade, na aceção do artigo 2.º, ponto 57), da Diretiva (UE) 2019/944;
- b) Operadores nomeados do mercado da eletricidade, na aceção do artigo 2.º, ponto 8), do Regulamento (UE) 2019/943;
- c) Mercados organizados, na aceção do artigo 2.º, ponto 4), do Regulamento de Execução (UE) n.º 1348/2014 da Comissão ⁽¹⁴⁾, que organizam transações de produtos relevantes para os fluxos transfronteiriços de eletricidade;
- d) Prestadores de serviços de TIC críticos a que se refere o artigo 3.º, ponto 9), do presente regulamento;
- e) A REORT para a Eletricidade criada nos termos do artigo 28.º do Regulamento (UE) 2019/943;
- f) A entidade ORDUE criada nos termos do artigo 52.º do Regulamento (UE) 2019/943;
- g) Agentes de mercado responsáveis pela liquidação de desvios, na aceção do artigo 2.º, ponto 14), do Regulamento (UE) 2019/943;
- h) Operadores de pontos de carregamento, na aceção do anexo I da Diretiva (UE) 2022/2555;
- i) Centros de coordenação regionais, conforme estabelecidos nos termos do artigo 35.º do Regulamento (UE) 2019/943;
- j) Prestadores de serviços de segurança geridos, na aceção do artigo 6.º, ponto 40), da Diretiva (UE) 2022/2555;
- k) Qualquer outra entidade ou terceiro aos quais tenham sido delegadas ou atribuídas responsabilidades nos termos do presente regulamento.

2. No âmbito dos seus atuais mandatos, as autoridades a seguir indicadas são responsáveis pelo exercício das funções que lhes são atribuídas pelo presente regulamento:

- a) A Agência da União Europeia de Cooperação dos Reguladores da Energia (ACER) criada pelo Regulamento (UE) 2019/942 do Parlamento Europeu e do Conselho ⁽¹⁵⁾;
- b) As autoridades nacionais competentes responsáveis pelo exercício das funções que lhes são atribuídas ao abrigo do presente regulamento e designadas pelos Estados-Membros nos termos do artigo 4.º, ou «autoridade competente»;
- c) As entidades reguladoras nacionais (ERN) designadas por cada Estado-Membro nos termos do artigo 57.º, n.º 1, da Diretiva (UE) 2019/944;

⁽¹⁴⁾ Regulamento de Execução (UE) n.º 1348/2014 da Comissão, de 17 de dezembro de 2014, relativo à comunicação de dados que dá execução ao artigo 8.º, n.ºs 2 e 6, do Regulamento (UE) n.º 1227/2011 do Parlamento Europeu e do Conselho relativo à integridade e à transparência nos mercados grossistas da energia (JO L 363 de 18.12.2014, p. 121).

⁽¹⁵⁾ Regulamento (UE) 2019/942 do Parlamento Europeu e do Conselho, de 5 de junho de 2019, que institui a Agência da União Europeia de Cooperação dos Reguladores da Energia (JO L 158 de 14.6.2019, p. 22).

- d) As autoridades competentes em matéria de preparação para riscos estabelecidas nos termos do artigo 3.º do Regulamento (UE) 2019/941;
 - e) Equipas de resposta a incidentes de segurança informática (CSIRT) designadas ou criadas nos termos do artigo 10.º da Diretiva (UE) 2022/2555;
 - f) Autoridades competentes responsáveis pela cibersegurança designadas ou criadas nos termos do artigo 8.º da Diretiva (UE) 2022/2555;
 - g) A Agência da União Europeia para a Cibersegurança criada nos termos do Regulamento (UE) 2019/881;
 - h) Quaisquer outras autoridades ou terceiros aos quais tenham sido delegadas ou atribuídas responsabilidades nos termos do artigo 4.º, n.º 3.
3. O presente regulamento é igualmente aplicável a todas as entidades que não estejam estabelecidas na União, mas que prestem serviços a entidades na União, desde que tenham sido identificadas como entidades de impacto elevado ou crítico pelas autoridades competentes, em conformidade com o artigo 24.º, n.º 2.
4. O presente regulamento não prejudica a responsabilidade que incumbe aos Estados-Membros de salvaguardarem a segurança nacional nem os seus poderes para salvaguardar outras funções essenciais do Estado, nomeadamente garantir a integridade territorial do Estado e manter a ordem pública.
5. O presente regulamento não prejudica a responsabilidade que incumbe aos Estados-Membros de salvaguardarem a segurança nacional no que respeita às atividades de produção de eletricidade a partir de centrais nucleares, nomeadamente às atividades no âmbito da cadeia de valor nuclear, em conformidade com os Tratados.
6. As entidades, as autoridades competentes, os pontos de contacto únicos a nível das entidades e as CSIRT procedem ao tratamento dos dados pessoais na medida do necessário para efeitos do presente regulamento e em conformidade com o Regulamento (UE) 2016/679, devendo o tratamento basear-se, em especial, no artigo 6.º deste regulamento.

Artigo 3.º

Definições

São aplicáveis as seguintes definições:

- 1) «Ativo», qualquer informação, programa informático ou equipamento informático dos sistemas de rede e informação, tangível ou intangível, que tenha valor para uma pessoa, uma organização ou uma administração pública;
- 2) «Autoridade competente em matéria de preparação para riscos», uma autoridade competente designada nos termos do artigo 3.º do Regulamento (UE) 2019/941;
- 3) «Equipa de resposta a incidentes de segurança informática», uma equipa responsável pelo tratamento de riscos e incidentes em conformidade com o artigo 10.º da Diretiva (UE) 2022/2555;
- 4) «Ativo de impacto crítico», um ativo que é necessário para realizar um processo de impacto crítico;
- 5) «Entidade de impacto crítico», uma entidade que realiza um processo de impacto crítico e que é identificada pelas autoridades competentes em conformidade com o artigo 24.º;
- 6) «Perímetro de impacto crítico», um perímetro definido por uma entidade referida no artigo 2.º, n.º 1, que contém todos os ativos de impacto crítico, no qual o acesso a esses ativos pode ser controlado e que delimita o âmbito de aplicação dos controlos avançados de cibersegurança;
- 7) «Processo de impacto crítico», um processo operacional realizado por uma entidade cujos índices de impacto na cibersegurança da eletricidade estão acima do limiar de impacto crítico;
- 8) «Limiar de impacto crítico», os valores dos índices de impacto na cibersegurança da eletricidade referidos no artigo 19.º, n.º 3, alínea b), acima dos quais um ciberataque a um processo operacional provocará uma perturbação crítica dos fluxos transfronteiriços de eletricidade;
- 9) «Prestador de serviços de TIC crítico», uma entidade que presta um serviço de TIC ou um processo de TIC que é necessário para um processo de impacto crítico ou de impacto elevado que afete aspetos de cibersegurança dos fluxos transfronteiriços de eletricidade e que, se comprometido, pode provocar um ciberataque cujo impacto supere o limiar de impacto crítico ou de impacto elevado;
- 10) «Fluxo transfronteiriço de eletricidade», um fluxo transfronteiriço na aceção do artigo 2.º, ponto 3), do Regulamento (UE) 2019/943;
- 11) «Ciberataque», um incidente na aceção do artigo 3.º, ponto 14), do Regulamento (UE) 2022/2554;
- 12) «Cibersegurança», cibersegurança na aceção do artigo 2.º, ponto 1), do Regulamento (UE) 2019/881;

- 13) «Controlo da cibersegurança», as ações ou procedimentos realizados com o objetivo de evitar, detetar, combater ou minimizar os riscos de cibersegurança;
- 14) «Incidente de cibersegurança», um incidente na aceção do artigo 6.º, ponto 6), da Diretiva (UE) 2022/2555;
- 15) «Sistema de gestão da cibersegurança», as políticas, procedimentos, orientações e recursos e atividades associados, geridos coletivamente por uma entidade, com vista a proteger os seus ativos de informação contra ciberameaças, estabelecendo, executando, operando, monitorizando, analisando, mantendo e melhorando de forma sistemática a segurança do sistema de rede e informação de uma organização;
- 16) «Centro de operações de cibersegurança», um centro específico no qual uma equipa técnica composta por um ou mais peritos, apoiados por sistemas informáticos de cibersegurança, executa tarefas relacionadas com a segurança (serviços do centro de operações de cibersegurança), como o tratamento de ciberataques e erros de configuração de segurança, a monitorização da segurança, a análise de registos e a deteção de ciberataques;
- 17) «Ciberameaça», uma ciberameaça na aceção do artigo 2.º, ponto 8), do Regulamento (UE) 2019/881;
- 18) «Gestão das vulnerabilidades em matéria de cibersegurança», a prática de identificar e corrigir vulnerabilidades;
- 19) «Entidade», uma entidade na aceção do artigo 6.º, ponto 38), da Diretiva (UE) 2022/2555;
- 20) «Alerta precoce», as informações necessárias para indicar a suspeita de que o incidente significativo tenha sido provocado por atos ilícitos ou maliciosos ou possa ter um impacto transfronteiriço;
- 21) «Índice de impacto na cibersegurança da eletricidade», um índice ou escala de classificação que classifica as possíveis consequências dos ciberataques para os processos operacionais associados aos fluxos transfronteiriços de eletricidade;
- 22) «Sistema europeu de certificação da cibersegurança», um sistema na aceção do artigo 2.º, ponto 9), do Regulamento (UE) 2019/881;
- 23) «Entidade de impacto elevado», uma entidade que realiza um processo de impacto elevado e que é identificada pelas autoridades competentes em conformidade com o artigo 24.º;
- 24) «Processo de impacto elevado», qualquer processo operacional realizado por uma entidade cujos índices de impacto na cibersegurança da eletricidade estão acima do limiar de impacto elevado;
- 25) «Ativo de impacto elevado», um ativo que é necessário para a realização de um processo de impacto elevado;
- 26) «Limiar de impacto elevado», os valores dos índices de impacto na cibersegurança da eletricidade referidos no artigo 19.º, n.º 3, alínea b), acima dos quais um ciberataque bem-sucedido a um processo provocará uma perturbação elevada dos fluxos transfronteiriços de eletricidade;
- 27) «Perímetro de impacto elevado», um perímetro definido por uma entidade elencada no artigo 2.º, n.º 1, que contém todos os ativos de impacto elevado, no qual o acesso a esses ativos pode ser controlado e que delimita o âmbito de aplicação dos controlos mínimos de cibersegurança;
- 28) «Produto de TIC», um produto de TIC na aceção do artigo 2.º, ponto 12), do Regulamento (UE) 2019/881;
- 29) «Serviço de TIC», um serviço de TIC na aceção do artigo 2.º, ponto 13), do Regulamento (UE) 2019/881;
- 30) «Processo de TIC», um processo de TIC na aceção do artigo 2.º, ponto 14), do Regulamento (UE) 2019/881;
- 31) «Sistema legado», um sistema de TIC legado na aceção do artigo 3.º, ponto 3), do Regulamento (UE) 2022/2554;
- 32) «Ponto de contacto único nacional», o ponto de contacto único designado ou criado por cada Estado-Membro nos termos do artigo 8.º, n.º 3, da Diretiva (UE) 2022/2555;
- 33) «Autoridades de gestão de cibercrises do sistema de rede e informação», as autoridades designadas ou criadas nos termos do artigo 9.º, n.º 1, da Diretiva (UE) 2022/2555;
- 34) «Iniciador», uma entidade que inicia um evento de intercâmbio, de partilha ou de armazenamento de informações;
- 35) «Caderno de encargos», as especificações que as entidades definem para a aquisição de produtos, processos ou serviços de TIC novos ou atualizados;
- 36) «Representante», uma pessoa singular ou coletiva estabelecida na União expressamente designada para agir em nome de uma entidade de impacto elevado ou de impacto crítico não estabelecida na União, mas que presta serviços a entidades na União e que pode ser contactada por uma autoridade competente ou por uma CSIRT em substituição da própria entidade de impacto elevado ou de impacto crítico no que respeita às obrigações dessa entidade nos termos do presente regulamento;

- 37) «Risco», um risco na aceção do artigo 6.º, ponto 9), da Diretiva (UE) 2022/2555;
- 38) «Matriz de impacto do risco», uma matriz utilizada durante a avaliação dos riscos para determinar o nível de impacto do risco para cada risco avaliado;
- 39) «Crise de eletricidade simultânea», uma crise de eletricidade na aceção do artigo 2.º, ponto 10), do Regulamento (UE) 2019/941;
- 40) «Ponto de contacto único a nível da entidade», ponto de contacto único a nível da entidade designado nos termos do artigo 38.º, n.º 1, alínea c);
- 41) «Parte interessada», qualquer parte interessada no êxito e no funcionamento contínuo de uma organização ou processo, como trabalhadores, administradores, acionistas, reguladores, associações, fornecedores e clientes;
- 42) «Norma», uma norma na aceção do artigo 2.º, ponto 1), do Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho ⁽¹⁶⁾;
- 43) «Região de exploração da rede», as regiões de exploração da rede na aceção do anexo I da Decisão 05-2022 da ACER relativa à definição de regiões de exploração da rede, estabelecidas em conformidade com o artigo 36.º do Regulamento (UE) 2019/943;
- 44) «Operador de rede», qualquer «operador da rede de distribuição» (ORD) ou «operador da rede de transporte» (ORT) na aceção do artigo 2.º, pontos 29) e 35), da Diretiva (UE) 2019/944;
- 45) «Processo de impacto crítico à escala da União», qualquer processo do setor da eletricidade, possivelmente envolvendo várias entidades, em relação ao qual o eventual impacto de um ciberataque possa ser considerado crítico durante a realização da avaliação dos riscos de cibersegurança à escala da União;
- 46) «Processo de impacto elevado à escala da União», qualquer processo do setor da eletricidade, possivelmente envolvendo várias entidades, em relação ao qual o eventual impacto de um ciberataque possa ser considerado elevado durante a realização da avaliação dos riscos de cibersegurança à escala da União;
- 47) «Vulnerabilidade ativamente explorada não corrigida», uma vulnerabilidade que ainda não foi divulgada publicamente nem corrigida e relativamente à qual existem provas fiáveis de que um código malicioso foi executado por um interveniente num sistema sem autorização do proprietário do sistema;
- 48) «Vulnerabilidade», vulnerabilidade na aceção do artigo 6.º, ponto 15), da Diretiva (UE) 2022/2555.

Artigo 4.º

Autoridade competente

1. Logo que possível e, em qualquer caso, até 13 de dezembro de 2024, cada Estado-Membro deve designar uma autoridade governamental ou reguladora nacional responsável pelo exercício das funções que lhe são atribuídas pelo presente regulamento («autoridade competente»). Até ser designada a autoridade competente para exercer as funções previstas no presente regulamento, compete à entidade reguladora designada por cada Estado-Membro nos termos do artigo 57.º, n.º 1, da Diretiva (UE) 2019/944 exercer as funções de autoridade competente em conformidade com o presente regulamento.

2. Os Estados-Membros devem notificar sem demora a Comissão, a ACER, a ENISA, o grupo de cooperação SRI criado nos termos do artigo 14.º da Diretiva (UE) 2022/2555 e o Grupo de Coordenação da Eletricidade instituído nos termos do artigo 1.º da Decisão da Comissão de 15 de novembro de 2012 ⁽¹⁷⁾ e comunicar-lhes o nome e os dados de contacto da respetiva autoridade competente designada nos termos do n.º 1 do presente artigo, bem como quaisquer alterações subsequentes dos mesmos.

⁽¹⁶⁾ Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativo à normalização europeia, que altera as Diretivas 89/686/CEE e 93/15/CEE do Conselho e as Diretivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE do Parlamento Europeu e do Conselho e revoga a Decisão 87/95/CEE do Conselho e a Decisão n.º 1673/2006/CE do Parlamento Europeu e do Conselho (JO L 316 de 14.11.2012, p. 12).

⁽¹⁷⁾ Decisão da Comissão, de 15 de novembro de 2012, que institui o Grupo de Coordenação da Eletricidade (2012/C 353/02) (JO C 353 de 17.11.2012, p. 2).

3. Os Estados-Membros podem autorizar a respetiva autoridade competente a delegar as funções que lhe são atribuídas pelo presente regulamento noutras autoridades nacionais, com exceção das funções enumeradas no artigo 5.º. Cada autoridade competente acompanha a aplicação do presente regulamento pelas autoridades nas quais delegou funções. A autoridade competente comunica à Comissão, à ACER, ao Grupo de Coordenação da Eletricidade, à ENISA e ao grupo de cooperação SRI o nome, os dados de contacto, as funções atribuídas e quaisquer alterações subsequentes das autoridades às quais delegou funções.

Artigo 5.º

Cooperação entre as autoridades e os organismos competentes a nível nacional

As autoridades competentes devem coordenar e assegurar uma cooperação adequada entre as autoridades competentes responsáveis pela cibersegurança, as autoridades de gestão de cibersegurança, as ERN, as autoridades competentes em matéria de preparação para riscos e as CSIRT para efeitos do cumprimento das obrigações pertinentes estabelecidas no presente regulamento. As autoridades competentes devem também coordenar-se com quaisquer outros organismos ou autoridades conforme determinado por cada Estado-Membro, a fim de assegurar procedimentos eficientes e evitar a duplicação de funções e de obrigações. As autoridades competentes devem poder instruir as respetivas ERN no sentido de solicitarem à ACER um parecer nos termos do artigo 8.º, n.º 3.

Artigo 6.º

Termos e condições ou metodologias ou planos

1. Os ORT devem elaborar, em cooperação com a entidade ORDUE, propostas de termos e condições ou metodologias em conformidade com o n.º 2 ou de planos em conformidade com o n.º 3.
2. Os seguintes termos e condições ou metodologias e quaisquer alterações dos mesmos carecem de aprovação de todas as autoridades competentes:
 - a) As metodologias de avaliação dos riscos de cibersegurança previstas no artigo 18.º, n.º 1;
 - b) O relatório global de avaliação dos riscos de cibersegurança da eletricidade transfronteiriça previsto no artigo 23.º;
 - c) Os controlos de cibersegurança mínimos e avançados previstos no artigo 29.º e o levantamento dos controlos de cibersegurança da eletricidade com base em normas previsto no artigo 34.º, incluindo controlos de cibersegurança mínimos e avançados na cadeia de abastecimento, em conformidade com o artigo 33.º;
 - d) Uma recomendação relativa à contratação no domínio da cibersegurança prevista no artigo 35.º;
 - e) A metodologia da escala de classificação de ciberataques prevista no artigo 37.º, n.º 8.
3. As propostas de planos regionais de atenuação dos riscos de cibersegurança previstas no artigo 22.º devem ser aprovadas por todas as autoridades competentes da região de exploração da rede em causa.
4. As propostas de termos e condições ou metodologias enumeradas no n.º 2 ou de planos referidas no n.º 3 devem incluir uma proposta de calendário para a sua execução e uma descrição do impacto previsto nos objetivos do presente regulamento.
5. A entidade ORDUE pode apresentar um parecer fundamentado aos ORT em causa até três semanas antes do termo do prazo para a apresentação da proposta de termos e condições ou metodologias ou de planos às autoridades competentes. Os ORT responsáveis pela proposta de termos e condições ou metodologias ou de planos devem ter em conta o parecer fundamentado da entidade ORDUE antes da apresentação da proposta para aprovação pelas autoridades competentes. Os ORT devem fundamentar os casos nos quais o parecer da entidade ORDUE não seja tido em conta.
6. Na elaboração conjunta de termos, condições e metodologias e de planos, os ORT participantes devem cooperar de forma estreita. Os ORT, com o apoio da REORT para a Eletricidade e em cooperação com a entidade ORDUE, devem informar periodicamente as autoridades competentes e a ACER sobre os progressos realizados na elaboração dos termos e condições ou metodologias ou dos planos.

*Artigo 7.º***Regras de votação nos ORT**

1. Caso os ORT aos quais incumba decidir sobre propostas de termos e condições ou metodologias não consigam chegar a acordo, devem decidir por maioria qualificada. A maioria qualificada para essas propostas é calculada do seguinte modo:

- a) Constituída por ORT que representem, pelo menos, 55 % dos Estados-Membros; e
- b) ORT que representem um conjunto de Estados-Membros cuja população seja igual ou superior a 65 % da população da União.

2. A minoria de bloqueio para decisões sobre propostas de termos e condições ou de metodologias referidos no artigo 6.º, n.º 2, é composta por ORT que representem, pelo menos, quatro Estados-Membros; caso contrário, considera-se alcançada a maioria qualificada.

3. Caso os ORT de uma região de exploração da rede aos quais incumba decidir sobre propostas de planos referidas no artigo 6.º, n.º 2, não consigam chegar a acordo e caso a região de exploração da rede em causa abranja mais de cinco Estados-Membros, os ORT devem decidir por maioria qualificada. A maioria qualificada para a adoção das propostas a que se refere o artigo 6.º, n.º 2, é uma maioria:

- a) Constituída por ORT que representem, pelo menos, 72 % dos Estados-Membros em causa; e
- b) ORT que representem um conjunto de Estados-Membros cuja população seja igual ou superior a 65 % da população da região em causa.

4. A minoria de bloqueio para decisões sobre propostas de planos deve incluir ORT que representem mais de 35 % da população dos Estados-Membros participantes e ainda ORT que representem, pelo menos, mais um Estado-Membro em causa; se tal não se verificar, considera-se que foi alcançada uma maioria qualificada.

5. Nas decisões de ORT sobre propostas de termos e condições ou metodologias em conformidade com o artigo 6.º, n.º 2, cada Estado-Membro tem direito a um voto. Caso existam dois ou mais ORT no território de determinado Estado-Membro, este deve repartir os direitos de voto pelos ORT.

6. Se os ORT, em cooperação com a entidade ORDUE, não apresentarem às autoridades competentes relevantes uma proposta inicial ou alterada de termos e condições ou metodologias, ou de planos, nos prazos estabelecidos no presente regulamento, devem apresentar às autoridades competentes relevantes e à ACER os projetos pertinentes dos termos, condições e metodologias ou dos planos. Devem explicar o que impediu um acordo. As autoridades competentes devem tomar em conjunto as medidas adequadas para a adoção dos termos e condições ou metodologias exigidos ou dos planos exigidos. Tal pode ser feito, por exemplo, solicitando alterações aos projetos nos termos do presente número, revendo e completando esses projetos ou, caso não tenham sido apresentados projetos, definindo e aprovando os termos e condições ou metodologias exigidos ou os planos exigidos.

*Artigo 8.º***Apresentação de propostas às autoridades competentes**

1. Os ORT devem apresentar às autoridades competentes relevantes as propostas de termos e condições ou metodologias ou de planos para aprovação nos respetivos prazos estabelecidos nos artigos 18.º, 23.º, 29.º, 33.º, 34.º, 35.º e 37.º. As autoridades competentes podem prorrogar em conjunto esses prazos em circunstâncias excecionais, nomeadamente nos casos em que um prazo não possa ser cumprido devido a circunstâncias externas à esfera dos ORT ou da entidade ORDUE.

2. As propostas de termos e condições ou metodologias ou de planos a que se refere o n.º 1 devem ser comunicadas à ACER, para informação, ao mesmo tempo que forem apresentadas às autoridades competentes.

3. Mediante pedido conjunto das ERN, a ACER emite um parecer sobre a proposta de termos e condições ou metodologias ou de planos no prazo de seis meses após a receção da mesma e comunica esse parecer às ERN e às autoridades competentes. As ERN, as autoridades competentes responsáveis pela cibersegurança e quaisquer outras autoridades designadas como autoridades competentes devem coordenar-se entre si antes de as ERN solicitarem um parecer à ACER. A ACER pode incluir recomendações nesse parecer. A ACER deve consultar a ENISA antes de emitir um parecer sobre as propostas enumeradas no artigo 6.º, n.º 2.
4. As autoridades competentes devem consultar-se, cooperar estreitamente e coordenar-se entre si, a fim de chegarem a acordo sobre os termos e condições ou metodologias ou planos propostos. Antes de aprovarem os termos e condições ou metodologias ou os planos, devem rever e completar as propostas, se for caso disso, após consulta da REORT para a Eletricidade e da entidade ORDUE, a fim de assegurarem que as propostas estão em conformidade com o presente regulamento e contribuem para um nível comum de cibersegurança elevado em toda a União.
5. As autoridades competentes devem decidir sobre os termos e condições ou metodologias ou os planos no prazo de seis meses após a autoridade competente relevante ou, se for caso disso, a última autoridade competente relevante em causa receber os termos, condições e metodologias ou os planos.
6. Caso a ACER emita um parecer, as autoridades competentes relevantes devem tê-lo em consideração e tomar as suas decisões no prazo de seis meses após a receção do mesmo.
7. Caso as autoridades competentes exijam em conjunto uma alteração dos termos e condições ou metodologias propostos ou dos planos para os aprovarem, os ORT devem elaborar, em cooperação com a entidade ORDUE, uma proposta de alteração dos termos, condições e metodologias ou dos planos correspondente. Os ORT devem apresentar a proposta alterada para aprovação no prazo de dois meses após o pedido das autoridades competentes. As autoridades competentes devem decidir sobre a alteração dos termos e condições ou metodologias ou dos planos no prazo máximo de dois meses após a apresentação dos mesmos.
8. Caso as autoridades competentes não tenham conseguido chegar a acordo no prazo referido nos n.ºs 5 ou 7, informam desse facto a Comissão. A Comissão pode tomar medidas adequadas para tornar possível a adoção dos termos e condições ou metodologias ou dos planos exigidos.
9. Os ORT, com o apoio da REORT para a Eletricidade, e a entidade ORDUE devem publicar os termos e condições ou metodologias ou os planos nos respetivos sítios Web, após aprovação pelas autoridades competentes relevantes, salvo se essas informações forem consideradas confidenciais em conformidade com o artigo 47.º.
10. As autoridades competentes podem solicitar em conjunto aos ORT e à entidade ORDUE propostas de alteração dos termos e condições ou metodologias aprovados ou dos planos aprovados e determinar um prazo para a apresentação dessas propostas. Os ORT, em cooperação com a entidade ORDUE, também podem propor alterações às autoridades competentes por iniciativa própria. As propostas de alteração dos termos e condições ou metodologias ou dos planos devem ser elaboradas e aprovadas nos termos do presente artigo.
11. Pelo menos de três em três anos após a primeira adoção dos respetivos termos e condições ou metodologias ou planos, os ORT, em cooperação com a entidade ORDUE, devem analisar a eficácia dos termos e condições ou metodologias adotados ou dos planos adotados e comunicar as conclusões da análise às autoridades competentes e à ACER, sem demora injustificada.

Artigo 9.º

Consulta

1. Os ORT, com o apoio da REORT para a Eletricidade e em cooperação com a entidade ORDUE, devem consultar as partes interessadas, incluindo a ACER, a ENISA e a autoridade competente de cada Estado-Membro, sobre os projetos de propostas de termos e condições ou metodologias enumerados no artigo 6.º, n.º 2, e de planos referidos no artigo 6.º, n.º 3. A consulta deve decorrer durante um período não inferior a um mês.

2. As propostas de termos e condições ou metodologias enumeradas no artigo 6.º, n.º 2, apresentadas pelos ORT em cooperação com a entidade ORDUE, devem ser publicadas e submetidas a consulta a nível da União. As propostas de planos enumeradas no artigo 6.º, n.º 3, apresentadas a nível regional pelos ORT pertinentes em cooperação com a entidade ORDUE, devem ser submetidas a consulta, pelo menos, a nível regional.

3. Os ORT, com o apoio da REORT para a Eletricidade, e a entidade ORDUE responsável pela proposta de termos e condições ou metodologias ou de planos devem ter devidamente em conta os pontos de vista das partes interessadas resultantes das consultas realizadas em conformidade com o n.º 1, antes da sua apresentação para aprovação regulamentar. Em todos os casos, deve ser elaborada e oportunamente publicada, antes ou com a publicação da proposta de termos e condições ou metodologias, uma justificação sólida dos motivos da incorporação ou não incorporação, no documento apresentado, dos pontos de vista resultantes da consulta.

Artigo 10.º

Participação das partes interessadas

A ACER, em estreita cooperação com a REORT para a Eletricidade e a entidade ORDUE, deve organizar a participação das partes interessadas, nomeadamente reuniões periódicas com partes interessadas para identificar problemas e propor melhorias relacionadas com a aplicação do presente regulamento.

Artigo 11.º

Recuperação de custos

1. Os custos suportados pelos ORT e pelos ORD sujeitos a regulação das tarifas de rede e decorrentes das obrigações previstas no presente regulamento, incluindo os custos suportados pela REORT para a Eletricidade e pela entidade ORDUE, devem ser avaliados pela ERN competente de cada Estado-Membro.

2. Os custos avaliados como razoáveis, eficientes e proporcionados devem ser recuperados por meio de tarifas de rede ou de outros mecanismos adequados, conforme determinado pela ERN competente.

3. A pedido das ERN competentes, os ORT e os ORD referidos no n.º 1 devem, num prazo razoável determinado pela ERN, fornecer as informações necessárias para facilitar a avaliação dos custos incorridos.

Artigo 12.º

Acompanhamento

1. A ACER deve acompanhar a aplicação do presente regulamento em conformidade com o artigo 32.º, n.º 1, do Regulamento (UE) 2019/943 e o artigo 4.º, n.º 2, do Regulamento (UE) 2019/942. Ao realizar este acompanhamento, a ACER pode cooperar com a ENISA e solicitar o apoio da REORT para a Eletricidade e da entidade ORDUE. A ACER deve informar periodicamente o Grupo de Coordenação da Eletricidade e o grupo de cooperação SRI sobre a aplicação do presente regulamento.

2. A ACER deve publicar um relatório pelo menos de três em três anos após a entrada em vigor do presente regulamento, a fim de:

- a) Analisar o estado da execução das medidas de gestão dos riscos de cibersegurança aplicáveis no que respeita às entidades de impacto elevado e de impacto crítico;
- b) Identificar a eventual necessidade de regras adicionais em matéria de requisitos comuns, planeamento, acompanhamento, elaboração de relatórios e gestão de crises, para prevenir riscos para o setor da eletricidade;
- c) Identificar domínios a melhorar para a revisão do presente regulamento ou determinar domínios não abrangidos e novas prioridades que possam surgir devido à evolução tecnológica.

3. Até 13 de junho de 2025, a ACER, em cooperação com a ENISA e após consulta da REORT para a Eletricidade e da entidade ORDUE, pode emitir orientações sobre as informações pertinentes a comunicar à ACER para efeitos de acompanhamento, bem como sobre o processo e a frequência da recolha, com base nos indicadores de desempenho definidos em conformidade com o n.º 5.

4. As autoridades competentes podem ter acesso às informações pertinentes na posse da ACER que esta tenha recolhido nos termos do presente artigo.
5. A ACER, em cooperação com a ENISA e com o apoio da REORT para a Eletricidade e da entidade ORDUE, deve emitir indicadores de desempenho não vinculativos para a avaliação da fiabilidade operacional relacionados com os aspetos de cibersegurança dos fluxos transfronteiriços de eletricidade.
6. As entidades enumeradas no artigo 2.º, n.º 1, do presente regulamento devem apresentar à ACER as informações necessárias para esta desempenhar as funções elencadas no n.º 2.

Artigo 13.º

Avaliação comparativa

1. Até 13 de junho de 2025, a ACER, em cooperação com a ENISA, elabora um guia não vinculativo de avaliação comparativa da cibersegurança. O guia deve explicar às ERN os princípios da avaliação comparativa dos controlos de cibersegurança aplicados nos termos do n.º 2 do presente artigo, tendo em conta os custos da execução dos controlos e a eficácia da função desempenhada pelos processos, produtos, serviços, sistemas e soluções utilizados para executar esses controlos. Ao elaborar o guia, a ACER deve ter em conta os relatórios de avaliação comparativa existentes. A ACER deve enviar o guia às ERN, para informação.
2. No prazo de 12 meses após a elaboração do guia de avaliação comparativa nos termos do n.º 1, as ERN devem realizar uma avaliação comparativa para aferir se os investimentos em curso em cibersegurança:
 - a) Atenuam os riscos com impacto nos fluxos transfronteiriços de eletricidade;
 - b) Produzem os resultados desejados e geram ganhos de eficiência para o desenvolvimento das redes de eletricidade;
 - c) São eficientes e estão integrados na contratação global de ativos e serviços.
3. Na avaliação comparativa, as ERN podem ter em conta o guia não vinculativo de avaliação comparativa da cibersegurança elaborado pela ACER e devem avaliar, em especial:
 - a) As despesas médias relacionadas com a cibersegurança para atenuar os riscos com impacto nos fluxos transfronteiriços de eletricidade, especialmente no que respeita às entidades de impacto elevado e de impacto crítico;
 - b) Em cooperação com a REORT para a Eletricidade e a entidade ORDUE, os preços médios dos serviços, sistemas e produtos de cibersegurança que contribuem em grande medida para o reforço e a manutenção das medidas de gestão dos riscos de cibersegurança nas diferentes regiões de exploração da rede;
 - c) A existência e o nível de comparabilidade dos custos e das funções dos serviços, sistemas e soluções de cibersegurança adequados para a aplicação do presente regulamento, identificando as eventuais medidas necessárias para promover a eficiência das despesas, em especial nos casos em que possam ser necessários investimentos tecnológicos em cibersegurança.
4. Quaisquer informações relacionadas com a avaliação comparativa devem ser tratadas em conformidade com os requisitos de classificação de dados do presente regulamento, os controlos mínimos de cibersegurança e o relatório de avaliação dos riscos de cibersegurança da eletricidade transfronteiriça. A avaliação comparativa referida nos n.ºs 2 e 3 não é tornada pública.
5. Sem prejuízo dos requisitos de confidencialidade previstos no artigo 47.º e da necessidade de proteger a segurança das entidades sujeitas às disposições do presente regulamento, a avaliação comparativa referida nos n.ºs 2 e 3 do presente artigo deve ser partilhada com todas as ERN, todas as autoridades competentes, a ACER, a ENISA e a Comissão.

*Artigo 14.º***Acordos com ORT de fora da União**

1. No prazo de 18 meses após a entrada em vigor do presente regulamento, os ORT de uma região de exploração da rede vizinha de um país terceiro devem procurar celebrar acordos com ORT do país terceiro vizinho que estejam em conformidade com a legislação aplicável da União e que estabeleçam as bases para a cooperação em matéria de proteção da cibersegurança e para os acordos de cooperação em matéria de cibersegurança com esses ORT.
2. Os ORT devem informar a autoridade competente dos acordos celebrados nos termos do n.º 1.

*Artigo 15.º***Representantes legais**

1. As entidades que não tenham um estabelecimento na União, mas que prestem serviços a entidades na União e tenham sido notificadas como sendo entidades de impacto elevado ou de impacto crítico em conformidade com o artigo 24.º, n.º 6, devem, no prazo de três meses após a notificação, designar por escrito um representante na União e informar desse facto a autoridade competente notificadora.
2. Esse representante é mandatado para ser contactado por qualquer autoridade competente ou por uma CSIRT na União em complemento ou em substituição da entidade de impacto elevado ou de impacto crítico no que respeita às obrigações da entidade nos termos do presente regulamento. A entidade de impacto elevado ou de impacto crítico deve dotar o seu representante legal dos poderes necessários e de recursos suficientes para garantir a sua cooperação eficiente e atempada com as autoridades competentes ou as CSIRT pertinentes.
3. O representante deve estar estabelecido num dos Estados-Membros nos quais a entidade oferece os seus serviços. Considera-se que a entidade está sob a jurisdição do Estado-Membro no qual o representante está estabelecido. As entidades de impacto elevado ou de impacto crítico comunicam o nome, o endereço postal, o endereço de correio eletrónico e o número de telefone do seu representante legal à autoridade competente do Estado-Membro no qual esse representante legal resida ou se encontre estabelecido.
4. O representante legal designado pode ser considerado responsável pelo incumprimento das obrigações previstas no presente regulamento, sem prejuízo da responsabilidade da própria entidade de impacto elevado ou de impacto crítico e das ações judiciais que possam ser intentadas contra esta última.
5. Na ausência de um representante na União designado nos termos do presente artigo, qualquer Estado-Membro no qual a entidade preste serviços pode intentar ações judiciais contra essa entidade por incumprimento das obrigações decorrentes do presente regulamento.
6. A designação de um representante legal na União nos termos do n.º 1 não constitui um estabelecimento na União.

*Artigo 16.º***Cooperação entre a REORT para a Eletricidade e a entidade ORDUE**

1. A REORT para a Eletricidade e a entidade ORDUE devem cooperar na realização de avaliações dos riscos de cibersegurança nos termos do artigo 19.º e do artigo 21.º e, em especial, nas seguintes tarefas:
 - a) Desenvolvimento das metodologias de avaliação dos riscos de cibersegurança em conformidade com o artigo 18.º, n.º 1;
 - b) Elaboração do relatório global de avaliação dos riscos de cibersegurança da eletricidade transfronteiriça nos termos do artigo 23.º;
 - c) Criação do quadro comum de cibersegurança da eletricidade nos termos do capítulo III;
 - d) Elaboração da recomendação relativa à contratação no domínio da cibersegurança nos termos do artigo 35.º;

- e) Criação da metodologia da escala de classificação de ciberataques em conformidade com o artigo 37.º, n.º 8;
 - f) Desenvolvimento do índice provisório de impacto na cibersegurança da eletricidade nos termos do artigo 48.º, n.º 1, alínea a);
 - g) Elaboração da lista provisória consolidada de entidades de impacto elevado e de impacto crítico nos termos do artigo 48.º, n.º 3;
 - h) Elaboração da lista provisória de processos de impacto elevado e de impacto crítico à escala da União, nos termos do artigo 48.º, n.º 4;
 - i) Elaboração da lista provisória de normas e controlos europeus e internacionais nos termos do artigo 48.º, n.º 6;
 - j) Realização da avaliação dos riscos de cibersegurança à escala da União nos termos do artigo 19.º;
 - k) Realização das avaliações regionais dos riscos de cibersegurança nos termos do artigo 21.º;
 - l) Definição dos planos regionais de atenuação dos riscos de cibersegurança nos termos do artigo 22.º;
 - m) Elaboração de orientações sobre sistemas europeus de certificação da cibersegurança de produtos, serviços e processos de TIC, em conformidade com o artigo 36.º;
 - n) Elaboração de orientações para a aplicação do presente regulamento, em consulta com a ACER e a ENISA.
2. A cooperação entre a REORT para a Eletricidade e a entidade ORDUE pode assumir a forma de um grupo de trabalho sobre os riscos de cibersegurança.
3. A REORT para a Eletricidade e a entidade ORDUE devem informar periodicamente a ACER, a ENISA, o grupo de cooperação SRI e o Grupo de Coordenação da Eletricidade sobre os progressos realizados na execução das avaliações dos riscos de cibersegurança a nível regional e à escala da União, nos termos dos artigos 19.º e 21.º.

Artigo 17.º

Cooperação entre a ACER e as autoridades competentes

A ACER, em cooperação com cada autoridade competente, deve:

- 1) Acompanhar a aplicação das medidas de gestão dos riscos de cibersegurança nos termos do artigo 12.º, n.º 2, alínea a), e das obrigações de elaboração de relatórios nos termos dos artigos 27.º e 39.º;
- 2) Acompanhar o processo de adoção e a aplicação dos termos e condições ou metodologias ou dos planos, nos termos do artigo 6.º, n.ºs 2 e 3. A cooperação entre a ACER, a ENISA e cada autoridade competente pode assumir a forma de um organismo de acompanhamento dos riscos de cibersegurança.

CAPÍTULO II

AValiação dos riscos e identificação dos riscos de cibersegurança pertinentes

Artigo 18.º

Metodologias de avaliação dos riscos de cibersegurança

- 1. Até 13 de março de 2025, os ORT, com o apoio da REORT para a Eletricidade, em cooperação com a entidade ORDUE e após consulta do grupo de cooperação SRI, devem apresentar uma proposta de metodologias de avaliação dos riscos de cibersegurança à escala da União, a nível regional e dos Estados-Membros.
- 2. As metodologias de avaliação dos riscos de cibersegurança à escala da União, a nível regional e dos Estados-Membros devem incluir:
 - a) Uma lista de ciberameaças a considerar, incluindo, pelo menos, as seguintes ameaças à cadeia de abastecimento:
 - i) degradação grave e inesperada da cadeia de abastecimento,
 - ii) indisponibilidade de produtos, serviços ou processos de TIC da cadeia de abastecimento,

- iii) ciberataques iniciados por intervenientes na cadeia de abastecimento,
 - iv) fugas de informações sensíveis ao longo da cadeia de abastecimento, incluindo a monitorização da cadeia de abastecimento,
 - v) introdução de fragilidades ou falhas de segurança (*backdoors*) nos produtos, serviços ou processos de TIC por intervenientes na cadeia de abastecimento;
- b) Os critérios para avaliar o impacto dos riscos de cibersegurança como elevados ou críticos, utilizando limiares definidos para as consequências e a probabilidade;
- c) Uma abordagem para analisar os riscos de cibersegurança decorrentes de sistemas legados, os efeitos em cascata dos ciberataques e a natureza em tempo real dos sistemas que operam a rede;
- d) Uma abordagem para analisar os riscos de cibersegurança decorrentes da dependência de um único fornecedor de produtos, serviços ou processos de TIC.
3. As metodologias de avaliação dos riscos de cibersegurança à escala da União, a nível regional e dos Estados-Membros devem avaliar os riscos de cibersegurança utilizando a mesma matriz de impacto do risco. A matriz de impacto do risco deve:
- a) Medir as consequências dos ciberataques com base nos seguintes critérios:
 - i) perda de carga,
 - ii) redução da produção de eletricidade,
 - iii) perda de capacidade na reserva de frequência primária,
 - iv) perda de capacidade para restabelecer o funcionamento de uma rede elétrica sem depender da rede de transporte externa para recuperar após uma paragem total ou parcial (também designada por «arranque autónomo»),
 - v) a duração prevista de uma indisponibilidade de eletricidade que afeta os clientes em combinação com a escala da indisponibilidade em número de clientes,
 - vi) quaisquer outros critérios quantitativos ou qualitativos que possam razoavelmente servir de indicador do efeito de um ciberataque nos fluxos transfronteiriços de eletricidade;
 - b) Medir a probabilidade de um incidente, como a frequência de ciberataques por ano.
4. As metodologias de avaliação dos riscos de cibersegurança à escala da União devem descrever a forma como serão definidos os valores do índice de impacto na cibersegurança da eletricidade para os limiares de impacto elevado e de impacto crítico. O índice de impacto na cibersegurança da eletricidade deve permitir às entidades estimar, com base nos critérios a que se refere o n.º 2, alínea b), o impacto dos riscos no seu processo operacional durante as avaliações de impacto operacional que realizam nos termos do artigo 26.º, n.º 4, alínea c), subalínea i).
5. A REORT para a Eletricidade, em coordenação com a entidade ORDUE, deve informar o Grupo de Coordenação da Eletricidade sobre as propostas de metodologias de avaliação dos riscos de cibersegurança elaboradas nos termos do n.º 1.

Artigo 19.º

Avaliação dos riscos de cibersegurança à escala da União

1. No prazo de nove meses após a aprovação das metodologias de avaliação dos riscos de cibersegurança nos termos do artigo 8.º e, posteriormente, de três em três anos, a REORT para a Eletricidade, em cooperação com a entidade ORDUE e em consulta com o grupo de cooperação SRI, deve, sem prejuízo do disposto no artigo 22.º da Diretiva (UE) 2022/2555, realizar uma avaliação dos riscos de cibersegurança à escala da União e elaborar um projeto de relatório de avaliação dos riscos de cibersegurança à escala da União. Para o efeito, serão utilizadas as metodologias criadas nos termos do artigo 18.º e aprovadas nos termos do artigo 8.º, para identificar, analisar e avaliar as possíveis consequências dos ciberataques que afetam a segurança operacional da rede de eletricidade e perturbam os fluxos transfronteiriços de eletricidade. A avaliação dos riscos de cibersegurança à escala da União não deve ter em conta os danos jurídicos, financeiros ou reputacionais provocados pelos ciberataques.
2. O relatório de avaliação dos riscos de cibersegurança à escala da União deve incluir os seguintes elementos:
- a) Os processos de impacto elevado e de impacto crítico à escala da União;
 - b) Uma matriz de impacto do risco que as entidades e as autoridades competentes devem utilizar para avaliar o risco de cibersegurança identificado na avaliação dos riscos de cibersegurança a nível do Estado-Membro realizada nos termos do artigo 20.º e na avaliação dos riscos de cibersegurança a nível da entidade nos termos do artigo 26.º, n.º 2, alínea b).

3. No que respeita aos processos de impacto elevado e de impacto crítico à escala da União, o relatório de avaliação dos riscos de cibersegurança à escala da União deve incluir:
 - a) Uma avaliação das possíveis consequências de um ciberataque utilizando os parâmetros definidos na metodologia de avaliação dos riscos de cibersegurança elaborada nos termos do artigo 18.º, n.ºs 2, 3 e 4, e aprovada nos termos do artigo 8.º;
 - b) O índice de impacto na cibersegurança da eletricidade e os limiares de impacto elevado e de impacto crítico que as autoridades competentes devem utilizar nos termos do artigo 24.º, n.ºs 1 e 2, para identificar as entidades de impacto elevado e de impacto crítico que intervêm nos processos de impacto elevado e de impacto crítico à escala da União.
4. A REORT para a Eletricidade, em cooperação com a entidade ORDUE, deve apresentar à ACER, para parecer, o projeto de relatório de avaliação dos riscos de cibersegurança à escala da União com os resultados da avaliação dos riscos de cibersegurança à escala da União. A ACER deve emitir um parecer sobre o projeto de relatório no prazo de três meses após a sua receção. Ao finalizarem esse relatório, a REORT para a Eletricidade e a entidade ORDUE devem ter na máxima consideração o parecer da ACER.
5. No prazo de três meses após a receção do parecer da ACER, a REORT para a Eletricidade em cooperação com a entidade ORDUE deve informar a ACER, a Comissão, a ENISA e as autoridades competentes sobre o relatório final de avaliação dos riscos de cibersegurança à escala da União.

Artigo 20.º

Avaliação dos riscos de cibersegurança a nível dos Estados-Membros

1. Cada autoridade competente deve realizar uma avaliação dos riscos de cibersegurança a nível de um Estado-Membro para todas as entidades de impacto elevado e de impacto crítico no seu Estado-Membro, utilizando as metodologias desenvolvidas nos termos do artigo 18.º e aprovadas nos termos do artigo 8.º. A avaliação dos riscos de cibersegurança a nível de um Estado-Membro identifica e analisa os riscos de ciberataques que afetam a segurança operacional da rede de eletricidade e que perturbam os fluxos transfronteiriços de eletricidade. A avaliação dos riscos de cibersegurança a nível de um Estado-Membro não deve ter em conta os danos jurídicos, financeiros ou reputacionais provocados pelos ciberataques.
2. No prazo de 21 meses após a notificação das entidades de impacto elevado e de impacto crítico nos termos do artigo 24.º, n.º 6, e de três em três anos após essa data, bem como na sequência da consulta à autoridade competente responsável pela cibersegurança no domínio da eletricidade, cada autoridade competente, apoiada pela CSIRT, deve apresentar um relatório de avaliação dos riscos de cibersegurança a nível do Estado-Membro à REORT para a Eletricidade e à entidade ORDUE, contendo as seguintes informações relativas a cada processo operacional de impacto elevado e de impacto crítico:
 - a) O estado da execução dos controlos de cibersegurança mínimos e avançados nos termos do artigo 29.º;
 - b) Uma lista de todos os ciberataques comunicados nos três anos anteriores nos termos do artigo 38.º, n.º 3;
 - c) Um resumo das informações sobre ciberameaças comunicadas nos três anos anteriores nos termos do artigo 38.º, n.º 6;
 - d) Para cada processo de impacto elevado ou de impacto crítico à escala da União, uma estimativa dos riscos de comprometimento da confidencialidade, integridade e disponibilidade das informações e dos ativos pertinentes;
 - e) Se necessário, uma lista de outras entidades identificadas como de impacto elevado ou de impacto crítico nos termos do artigo 24.º, n.ºs 1, 2, 3 e 5.
3. O relatório de avaliação dos riscos de cibersegurança a nível do Estado-Membro deve ter em conta o plano de preparação para riscos do Estado-Membro, estabelecido nos termos do artigo 10.º do Regulamento (UE) 2019/941.
4. As informações contidas no relatório de avaliação dos riscos de cibersegurança a nível do Estado-Membro nos termos do n.º 2, alíneas a) a d), não podem estar ligadas a entidades ou ativos específicos. O relatório de avaliação dos riscos de cibersegurança a nível do Estado-Membro deve incluir também uma avaliação dos riscos das derrogações temporárias emitidas pelas autoridades competentes dos Estados-Membros nos termos do artigo 30.º.

5. A REORT para a Eletricidade e a entidade ORDUE podem solicitar informações adicionais às autoridades competentes relativamente às funções especificadas no n.º 2, alíneas a) e c).
6. As autoridades competentes devem assegurar que as informações que fornecem são exatas e corretas.

Artigo 21.º

Avaliações regionais dos riscos de segurança

1. A REORT para a Eletricidade, em cooperação com a entidade ORDUE e em consulta com o centro de coordenação regional competente, deve realizar uma avaliação regional dos riscos de cibersegurança para cada região de exploração da rede, utilizando as metodologias desenvolvidas nos termos do artigo 19.º e aprovadas nos termos do artigo 8.º, para identificar, analisar e avaliar os riscos de ciberataques que afetam a segurança operacional da rede de eletricidade e perturbam os fluxos transfronteiriços de eletricidade. As avaliações regionais dos riscos de cibersegurança não devem ter em conta os danos jurídicos, financeiros ou reputacionais provocados pelos ciberataques.
2. No prazo de 30 meses após a notificação das entidades de impacto elevado e de impacto crítico nos termos do artigo 24.º, n.º 6, e posteriormente de três em três anos, a REORT para a Eletricidade, em cooperação com a entidade ORDUE e em consulta com o grupo de cooperação SRI, deve elaborar um relatório da avaliação regional dos riscos de cibersegurança para cada região de exploração da rede.
3. O relatório da avaliação regional dos riscos de cibersegurança deve ter em conta as informações pertinentes contidas nos relatórios de avaliação dos riscos de cibersegurança à escala da União e nos relatórios de avaliação dos riscos de cibersegurança a nível dos Estados-Membros.
4. A avaliação regional dos riscos de cibersegurança deve ter em conta os cenários de crise de eletricidade regionais relacionados com a cibersegurança identificados nos termos do artigo 6.º do Regulamento (UE) 2019/941.

Artigo 22.º

Planos regionais de atenuação dos riscos de cibersegurança

1. No prazo de 36 meses após a notificação das entidades de impacto elevado e de impacto crítico nos termos do artigo 24.º, n.º 6, e o mais tardar até 13 de junho de 2031 e posteriormente de três em três anos, os ORT, com o apoio da REORT para a Eletricidade, em cooperação com a entidade ORDUE e em consulta com os centros de coordenação regionais e o grupo de cooperação SRI, devem elaborar um plano regional de atenuação dos riscos de cibersegurança para cada região de exploração da rede.
2. O plano regional de atenuação dos riscos de cibersegurança deve incluir:
 - a) Os controlos de cibersegurança mínimos e avançados que as entidades de impacto elevado e de impacto crítico devem aplicar na região de exploração da rede;
 - b) Os riscos de cibersegurança residuais nas regiões de exploração da rede após a aplicação dos controlos referidos na alínea a).
3. A REORT para a Eletricidade deve apresentar os planos regionais de atenuação dos riscos aos operadores da rede de transporte pertinentes, às autoridades competentes e ao Grupo de Coordenação da Eletricidade. O Grupo de Coordenação da Eletricidade pode recomendar alterações.
4. Os ORT, com o apoio da REORT para a Eletricidade, em cooperação com a entidade ORDUE e em consulta com o grupo de cooperação SRI, deve atualizar de três em três anos os planos regionais de atenuação dos riscos, salvo se as circunstâncias justificarem atualizações mais frequentes.

Artigo 23.º

Relatório global de avaliação dos riscos de cibersegurança da eletricidade transfronteiriça

1. No prazo de 40 meses após a notificação das entidades de impacto elevado e de impacto crítico nos termos do artigo 24.º, n.º 6, e posteriormente de três em três anos, os ORT, com o apoio da REORT para a Eletricidade, em cooperação com a entidade ORDUE e em consulta com o grupo de cooperação SRI, devem apresentar ao Grupo de Coordenação da Eletricidade um relatório sobre os resultados da avaliação dos riscos de cibersegurança no que respeita aos fluxos transfronteiriços de eletricidade («relatório global de avaliação dos riscos de cibersegurança da eletricidade transfronteiriça»).

2. O relatório global de avaliação dos riscos de cibersegurança da eletricidade transfronteiriça deve basear-se no relatório de avaliação dos riscos de cibersegurança à escala da União, nos relatórios de avaliação dos riscos de cibersegurança a nível dos Estados-Membros e nos relatórios das avaliações regionais dos riscos de cibersegurança, bem como incluir as seguintes informações:

- a) A lista de processos de impacto elevado e de impacto crítico à escala da União identificados no relatório de avaliação dos riscos de cibersegurança à escala da União, em conformidade com o artigo 19.º, n.º 2, alínea a), incluindo a estimativa da probabilidade e do impacto dos riscos de cibersegurança analisados durante os relatórios das avaliações regionais dos riscos de cibersegurança nos termos do artigo 21.º, n.º 2, e do artigo 19.º, n.º 3, alínea a);
- b) As ciberameaças atuais, com especial destaque para as ameaças emergentes e os riscos para a rede de eletricidade;
- c) Os ciberataques no período anterior à escala da União, fornecendo uma panorâmica crítica da forma como esses ciberataques podem ter tido impacto nos fluxos transfronteiriços de eletricidade;
- d) O estado geral da execução das medidas de cibersegurança;
- e) O estado da execução dos fluxos de informação nos termos dos artigos 37.º e 38.º;
- f) A lista de informações ou critérios específicos para a classificação das informações nos termos do artigo 46.º;
- g) Os riscos identificados e salientados que podem resultar de uma gestão insegura da cadeia de abastecimento;
- h) Os resultados e as experiências acumuladas de exercícios de cibersegurança regionais e transregionais organizados nos termos do artigo 44.º;
- i) Uma análise da evolução dos riscos globais de cibersegurança transfronteiriços no setor da eletricidade desde as últimas avaliações regionais dos riscos de cibersegurança;
- j) Quaisquer outras informações que possam ser úteis para identificar possíveis melhorias do presente regulamento ou a necessidade de uma revisão do presente regulamento ou de qualquer dos seus instrumentos;
- k) Informações agregadas e anonimizadas sobre as interrogações concedidas nos termos do artigo 30.º, n.º 3.

3. As entidades enumeradas no artigo 2.º, n.º 1, podem contribuir para a elaboração do relatório global de avaliação dos riscos de cibersegurança da eletricidade transfronteiriça, respeitando a confidencialidade das informações em conformidade com o artigo 47.º. Os ORT, com o apoio da REORT para a Eletricidade e em cooperação com a entidade ORDUE, devem consultar essas entidades desde uma fase inicial.

4. O relatório global de avaliação dos riscos de cibersegurança da eletricidade transfronteiriça está sujeito às regras em matéria de proteção do intercâmbio de informações nos termos do artigo 46.º. Sem prejuízo do artigo 10.º, n.º 4, e do artigo 47.º, n.º 4, a REORT para a Eletricidade e a entidade ORDUE devem divulgar uma versão pública desse relatório que não pode conter informações suscetíveis de causar danos às entidades enumeradas no artigo 2.º, n.º 1. A versão pública desse relatório só deve ser divulgada com o acordo do grupo de cooperação SRI e do Grupo de Coordenação da Eletricidade. A REORT para a Eletricidade, em coordenação com a entidade ORDUE, é responsável pela compilação e publicação da versão pública do relatório.

Artigo 24.º

Identificação de entidades de impacto elevado e de impacto crítico

1. Cada autoridade competente deve identificar, utilizando o índice de impacto na cibersegurança da eletricidade e os limiares de impacto elevado e de impacto crítico incluídos no relatório de avaliação dos riscos de cibersegurança à escala da União nos termos do artigo 19.º, n.º 3, alínea b), as entidades de impacto elevado e de impacto crítico no seu Estado-Membro que intervêm nos processos de impacto elevado e de impacto crítico à escala da União. As autoridades competentes podem solicitar informações a uma entidade do seu Estado-Membro para determinar os valores do índice de impacto na cibersegurança da eletricidade para essa entidade. Se o índice de impacto na cibersegurança da eletricidade determinado de uma entidade estiver acima do limiar de impacto elevado ou de impacto crítico, a entidade identificada deve ser incluída na lista constante do relatório de avaliação dos riscos de cibersegurança a nível do Estado-Membro referido no artigo 20.º, n.º 2.
2. Cada autoridade competente deve identificar, utilizando o índice de impacto na cibersegurança da eletricidade e os limiares de impacto elevado e de impacto crítico incluídos no relatório de avaliação dos riscos de cibersegurança à escala da União nos termos do artigo 19.º, n.º 3, alínea b), as entidades de impacto elevado e de impacto crítico não estabelecidas na União, desde que estejam ativas na União. A autoridade competente pode solicitar informações a uma entidade não estabelecida na União para determinar os valores do índice para essa entidade.
3. Cada autoridade competente pode identificar outras entidades no seu Estado-Membro como entidades de impacto elevado ou de impacto crítico se forem cumpridos os seguintes critérios:
 - a) A entidade faz parte de um grupo de entidades relativamente às quais existe um risco significativo de serem afetadas simultaneamente por um ciberataque;
 - b) O índice de impacto na cibersegurança da eletricidade agregado para todo o grupo de entidades está acima do limiar de impacto elevado ou de impacto crítico.
4. Se uma autoridade competente identificar outras entidades em conformidade com o n.º 3, todos os processos nessas entidades para os quais o índice de impacto na cibersegurança da eletricidade agregado para todo o grupo esteja acima do limiar de impacto elevado devem ser considerados processos de impacto elevado e todos os processos nessas entidades para os quais o índice de impacto na cibersegurança da eletricidade agregado para todo o grupo esteja acima dos limiares de impacto crítico devem ser considerados processos de impacto crítico.
5. Se uma autoridade competente identificar as entidades referidas no n.º 3, alínea a), em mais do que um Estado-Membro, deve informar as outras autoridades competentes, a REORT para a Eletricidade e a entidade ORDUE. A REORT para a Eletricidade, em cooperação com a entidade ORDUE, com base nas informações recebidas de todas as autoridades competentes, deve fornecer às autoridades competentes uma análise da agregação de entidades em mais do que um Estado-Membro que possa criar uma perturbação distribuída dos fluxos transfronteiriços de eletricidade e resultar num ciberataque. Caso um grupo de entidades em vários Estados-Membros seja identificado como uma agregação cujo índice de impacto na cibersegurança da eletricidade esteja acima do limiar de impacto elevado ou de impacto crítico, todas as autoridades competentes em causa devem identificar as entidades desse grupo como entidades de impacto elevado ou de impacto crítico para o respetivo Estado-Membro, com base no índice de impacto na cibersegurança da eletricidade agregado para o grupo de entidades, devendo as entidades identificadas ser incluídas na lista constante do relatório de avaliação dos riscos de cibersegurança à escala da União.
6. No prazo de nove meses após ter sido informada pela REORT para a Eletricidade e pela entidade ORDUE sobre relatório de avaliação dos riscos de cibersegurança à escala da União nos termos do artigo 19.º, n.º 5, e, em qualquer caso, o mais tardar até 13 de junho de 2028, cada autoridade competente deve informar as entidades constantes da lista de que foram identificadas como uma entidade de impacto elevado ou de impacto crítico no seu Estado-Membro.
7. Se um prestador de serviços for comunicado a uma autoridade competente como sendo prestador de serviços de TIC crítico nos termos do artigo 27.º, alínea c), essa autoridade competente deve notificá-lo às autoridades competentes dos Estados-Membros em cujo território está localizada a sede ou o representante. Esta última autoridade competente deve notificar o prestador de serviços de que foi identificado como prestador de serviços crítico.

*Artigo 25.º***Regimes nacionais de verificação**

1. As autoridades competentes podem criar um sistema nacional de verificação para verificar se as entidades de impacto crítico identificadas nos termos do artigo 24.º, n.º 1, aplicaram o quadro legislativo nacional incluído na matriz de mapeamento referida no artigo 34.º. O sistema nacional de verificação pode basear-se numa inspeção realizada pela autoridade competente, em auditorias de segurança independentes ou em avaliações mútuas pelos pares realizadas por entidades de impacto crítico no mesmo Estado-Membro, supervisionadas pela autoridade competente.
2. Se uma autoridade competente decidir criar um sistema nacional de verificação, deve assegurar que a verificação é efetuada em conformidade com os seguintes requisitos:
 - a) Qualquer parte que realize a avaliação pelos pares, a auditoria ou a inspeção deve ser independente da entidade de impacto crítico que esteja a ser verificada e não pode ter conflitos de interesses;
 - b) O pessoal que efetua a avaliação pelos pares, a auditoria ou a inspeção deve ter conhecimentos demonstráveis sobre:
 - i) cibersegurança no setor da eletricidade,
 - ii) sistemas de gestão da cibersegurança,
 - iii) os princípios em matéria de auditoria,
 - iv) avaliação dos riscos de cibersegurança,
 - v) o quadro comum de cibersegurança da eletricidade,
 - vi) o quadro legislativo e regulamentar nacional e as normas europeias e internacionais no âmbito da verificação,
 - vii) os processos de impacto crítico no âmbito da verificação;
 - c) A parte que realiza a avaliação pelos pares, a auditoria ou a inspeção deve dispor de tempo suficiente para realizar essas atividades;
 - d) A parte que realiza a avaliação pelos pares, a auditoria ou a inspeção deve tomar as medidas adequadas para proteger as informações que recolhe durante a verificação, em conformidade com o seu nível de confidencialidade;
 - e) As avaliações pelos pares, as auditorias ou as inspeções devem ser realizadas pelo menos uma vez por ano e abranger todo o âmbito da verificação pelo menos de três em três anos.
3. Se uma autoridade competente decidir criar um regime nacional de verificação, deve comunicar anualmente à ACER a frequência com que realiza inspeções ao abrigo desse regime.

*Artigo 26.º***Gestão dos riscos de cibersegurança a nível da entidade**

1. Cada entidade de impacto elevado e de impacto crítico identificada pelas autoridades competentes nos termos do artigo 24.º, n.º 1, deve realizar a gestão dos riscos de cibersegurança para todos os seus ativos nos seus perímetros de impacto elevado e de impacto crítico. Cada entidade de impacto elevado e de impacto crítico deve realizar, de três em três anos, uma gestão de riscos que inclua as fases referidas no n.º 2.
2. Cada entidade de impacto elevado e de impacto crítico deve basear a sua gestão dos riscos de cibersegurança numa abordagem que vise proteger a sua rede e sistemas de informação e que inclua as seguintes fases:
 - a) Estabelecimento do contexto;
 - b) Avaliação dos riscos de cibersegurança a nível da entidade;
 - c) Tratamento dos riscos de cibersegurança;
 - d) Aceitação dos riscos de cibersegurança.

3. Durante a fase de estabelecimento do contexto, cada entidade de impacto elevado e de impacto crítico deve:
 - a) Definir o âmbito da avaliação dos riscos de cibersegurança, incluindo os processos de impacto elevado e de impacto crítico identificados pela REORT para a Eletricidade e pela entidade ORDUE, bem como outros processos que possam ser alvo de ciberataques com impacto elevado ou crítico nos fluxos transfronteiriços de eletricidade;
 - b) Definir os critérios para a avaliação e aceitação dos riscos, em conformidade com a matriz de impacto do risco que as entidades e as autoridades competentes devem utilizar para avaliar os riscos de cibersegurança nas metodologias de avaliação dos riscos de cibersegurança à escala da União, a nível regional e a nível dos Estados-Membros desenvolvidas pela REORT para a Eletricidade e pela entidade ORDUE, em conformidade com o artigo 19.º, n.º 2.
4. Durante a fase de avaliação dos riscos de cibersegurança, cada entidade de impacto elevado e de impacto crítico deve:
 - a) Identificar os riscos de cibersegurança tendo em conta:
 - i) todos os ativos que apoiam processos de impacto elevado e de impacto crítico à escala da União, com uma avaliação do possível impacto nos fluxos transfronteiriços de eletricidade se o ativo estiver comprometido,
 - ii) eventuais ciberameaças, tendo em conta as ciberameaças identificadas no mais recente relatório global de avaliação dos riscos de cibersegurança da eletricidade transfronteiriça referido no artigo 23.º e as ameaças à cadeia de abastecimento,
 - iii) vulnerabilidades, incluindo vulnerabilidades nos sistemas legados,
 - iv) possíveis cenários de ciberataque, nomeadamente ciberataques que afetem a segurança operacional da rede de eletricidade e perturbem os fluxos transfronteiriços de eletricidade,
 - v) avaliações dos riscos pertinentes realizadas à escala da União, nomeadamente avaliações coordenadas dos riscos de cadeias de abastecimento críticas, em conformidade com o artigo 22.º da Diretiva (UE) 2022/2555, e
 - vi) controlos aplicados existentes;
 - b) Analisar a probabilidade e as consequências dos riscos de cibersegurança identificados na alínea a) e determinar o nível de risco de cibersegurança com recurso à matriz de impacto do risco utilizada para avaliar os riscos de cibersegurança nas metodologias de avaliação dos riscos de cibersegurança à escala da União, a nível regional e a nível dos Estados-Membros desenvolvidas pelos ORT, com o apoio da REORT para a Eletricidade e em cooperação com a entidade ORDUE, em conformidade com o artigo 19.º, n.º 2;
 - c) Classificar os ativos de acordo com as possíveis consequências caso a cibersegurança fique comprometida e determinar o perímetro de impacto elevado e de impacto crítico seguindo as seguintes etapas:
 - i) realizar, para todos os processos abrangidos pela avaliação dos riscos de cibersegurança, uma avaliação do impacto operacional utilizando o índice de impacto na cibersegurança da eletricidade,
 - ii) classificar um processo como de impacto elevado ou de impacto crítico se o seu índice de impacto na cibersegurança da eletricidade estiver acima do limiar de impacto elevado ou de impacto crítico, respetivamente,
 - iii) determinar todos os ativos de impacto elevado e de impacto crítico como os ativos necessários para os processos de impacto elevado e de impacto crítico, respetivamente,
 - iv) definir os perímetros de impacto elevado e de impacto crítico que contenham todos os ativos de impacto elevado e de impacto crítico, respetivamente, para que o acesso aos perímetros possa ser controlado;
 - d) Avaliar os riscos de cibersegurança, atribuindo-lhes prioridade por meio de critérios de avaliação dos riscos e de critérios de aceitação dos riscos referidos no n.º 3, alínea b).
5. Durante a fase de tratamento dos riscos de cibersegurança, cada entidade de impacto elevado e de impacto crítico deve criar um plano de atenuação dos riscos a nível da entidade, selecionando opções de tratamento de riscos adequadas para gerir os riscos e identificar os riscos residuais.
6. Durante a fase de aceitação dos riscos de cibersegurança, cada entidade de impacto elevado e de impacto crítico deve decidir se aceita o risco residual com base nos critérios de aceitação dos riscos estabelecidos no n.º 3, alínea b).

7. Cada entidade de impacto elevado e de impacto crítico deve registar os ativos identificados no n.º 1 num inventário de ativos. Esse inventário de ativos não faz parte do relatório de avaliação dos riscos.
8. Durante as inspeções, a autoridade competente pode examinar os ativos incluídos no inventário.

Artigo 27.º

Elaboração de relatórios sobre a avaliação dos riscos a nível das entidades

Cada entidade de impacto elevado e de impacto crítico deve, no prazo de 12 meses após a notificação das entidades de impacto elevado e de impacto crítico nos termos do artigo 24.º, n.º 6, e posteriormente de três em três anos, apresentar à autoridade competente um relatório com as seguintes informações:

- 1) Uma lista dos controlos selecionados para o plano de atenuação dos riscos a nível da entidade, em conformidade com o artigo 26.º, n.º 5, com o estado da execução atual de cada controlo;
- 2) Para cada processo de impacto elevado ou de impacto crítico à escala da União, uma estimativa do risco de comprometimento da confidencialidade, da integridade e da disponibilidade das informações e dos ativos pertinentes. A estimativa deste risco deve ser apresentada de acordo com a matriz de impacto do risco prevista no artigo 19.º, n.º 2;
- 3) Uma lista dos prestadores de serviços de TIC críticos para os seus processos de impacto crítico.

CAPÍTULO III

QUADRO COMUM DE CIBERSEGURANÇA DA ELETRICIDADE

Artigo 28.º

Composição, funcionamento e revisão do quadro comum de cibersegurança da eletricidade

1. O quadro comum de cibersegurança da eletricidade é composto pelos seguintes controlos e sistema de gestão da cibersegurança:
 - a) Os controlos de cibersegurança mínimos, desenvolvidos em conformidade com o artigo 29.º;
 - b) Os controlos de cibersegurança avançados, desenvolvidos em conformidade com o artigo 29.º;
 - c) A matriz de mapeamento, elaborada em conformidade com o artigo 34.º, que mapeia os controlos referidos nas alíneas a) e b) com base em normas europeias e internacionais e quadros legislativos ou regulamentares nacionais selecionados;
 - d) O sistema de gestão da cibersegurança criado nos termos do artigo 32.º.
2. Todas as entidades de impacto elevado devem aplicar no seu perímetro de impacto elevado os controlos de cibersegurança mínimos previstos no n.º 1, alínea a).
3. Todas as entidades de impacto crítico devem aplicar no seu perímetro de impacto elevado os controlos de cibersegurança avançados previstos no n.º 1, alínea b).
4. No prazo de sete meses após a apresentação do primeiro projeto de relatório de avaliação dos riscos de cibersegurança à escala da União nos termos do artigo 19.º, n.º 4, o quadro comum de cibersegurança da eletricidade a que se refere o n.º 1 deve ser complementado pelos controlos de cibersegurança mínimos e avançados da cadeia de abastecimento desenvolvidos nos termos do artigo 33.º.

*Artigo 29.º***Controlos de cibersegurança mínimos e avançados**

1. No prazo de sete meses após a apresentação do primeiro projeto de relatório de avaliação dos riscos de cibersegurança à escala da União nos termos do artigo 19.º, n.º 4, os ORT, com o apoio da REORT para a Eletricidade e em cooperação com a entidade ORDUE, devem elaborar uma proposta de controlos de cibersegurança mínimos e avançados.
2. No prazo de seis meses após a elaboração de cada relatório da avaliação regional dos riscos de cibersegurança nos termos do artigo 21.º, n.º 2, os ORT, com o apoio da REORT para a Eletricidade e em cooperação com a entidade ORDUE, devem propor à autoridade competente uma alteração dos controlos de cibersegurança mínimos e avançados. A proposta será elaborada em conformidade com o artigo 8.º, n.º 10, e terá em conta os riscos identificados na avaliação regional dos riscos.
3. Os controlos de cibersegurança mínimos e avançados devem ser verificáveis mediante a participação num sistema nacional de verificação em conformidade com o procedimento estabelecido no artigo 31.º ou mediante a realização de auditorias de segurança independentes por terceiros de acordo com os requisitos enumerados no artigo 25.º, n.º 2.
4. Os controlos de cibersegurança mínimos e avançados iniciais desenvolvidos nos termos do n.º 1 devem basear-se nos riscos identificados no relatório de avaliação dos riscos de cibersegurança à escala da União referido no artigo 19.º, n.º 5. Os controlos de cibersegurança mínimos e avançados alterados, elaborados nos termos do n.º 2, devem basear-se no relatório da avaliação regional dos riscos de cibersegurança referido no artigo 21.º, n.º 2.
5. Os controlos de cibersegurança mínimos devem incluir controlos destinados a proteger as informações trocadas nos termos do artigo 46.º.
6. No prazo de 12 meses após a aprovação dos controlos de cibersegurança mínimos e avançados nos termos do artigo 8.º, n.º 5, ou após cada atualização nos termos do artigo 8.º, n.º 10, as entidades enumeradas no artigo 2.º, n.º 1, e identificadas como entidades de impacto crítico e de impacto elevado nos termos do artigo 24.º devem, durante a elaboração do plano de atenuação dos riscos a nível da entidade nos termos do artigo 26.º, n.º 5, aplicar os controlos de cibersegurança mínimos no perímetro de impacto elevado e os controlos de cibersegurança avançados no perímetro de impacto crítico.

*Artigo 30.º***Derrogações aos controlos de cibersegurança mínimos e avançados**

1. As entidades enumeradas no artigo 2.º, n.º 1, podem solicitar à respetiva autoridade competente que conceda uma derrogação da sua obrigação de aplicar os controlos de cibersegurança mínimos e avançados referidos no artigo 29.º, n.º 6. A autoridade competente pode conceder essa derrogação por um dos seguintes motivos:
 - a) Em circunstâncias excecionais, se a entidade puder demonstrar que os custos da execução de controlos de cibersegurança adequados excedem significativamente os benefícios. A ACER e a REORT para a Eletricidade, em cooperação com a entidade ORDUE, podem elaborar conjuntamente orientações para estimar os custos dos controlos de cibersegurança, de forma a ajudar as entidades;
 - b) Se a entidade apresentar um plano de tratamento dos riscos a nível da entidade que atenua os riscos de cibersegurança utilizando controlos alternativos a um nível aceitável, de acordo com os critérios de aceitação de riscos referidos no artigo 26.º, n.º 3, alínea b).
2. Cada autoridade competente decide, no prazo de três meses a contar da receção do pedido a que se refere o n.º 1, se é concedida uma derrogação aos controlos de cibersegurança mínimos e avançados. As derrogações aos controlos de cibersegurança mínimos ou avançados são concedidas por um período máximo de três anos, com possibilidade de renovação.
3. As informações agregadas e anonimizadas relativas às derrogações concedidas devem ser incluídas num anexo do relatório global de avaliação dos riscos de cibersegurança da eletricidade transfronteiriça referido no artigo 23.º. A REORT para a Eletricidade e a entidade ORDUE devem atualizar conjuntamente a lista, caso seja necessário.

*Artigo 31.º***Verificação do quadro comum de cibersegurança da eletricidade**

1. O mais tardar 24 meses após a adoção dos controlos referidos no artigo 28.º, n.º 1, alíneas a), b) e c), e a criação do sistema de gestão da cibersegurança a que se refere a alínea d) do mesmo artigo, cada entidade de impacto crítico identificada nos termos do artigo 24.º, n.º 1, deve ser capaz de demonstrar, a pedido da autoridade competente, a sua conformidade com o sistema de gestão da cibersegurança e os controlos de cibersegurança mínimos ou avançados.
2. Cada entidade de impacto crítico deve cumprir a obrigação referida no n.º 1 submetendo-se a auditorias de segurança independentes realizadas por terceiros, em conformidade com os requisitos enumerados no artigo 25.º, n.º 2, ou participando num sistema nacional de verificação em conformidade com o artigo 25.º, n.º 1.
3. A verificação do cumprimento do sistema de gestão da cibersegurança e dos controlos de cibersegurança mínimos ou avançados por parte de uma entidade de impacto crítico deve abranger todos os ativos situados no perímetro de impacto crítico da entidade de impacto crítico.
4. A verificação do cumprimento do sistema de gestão da cibersegurança e dos controlos de cibersegurança mínimos ou avançados por parte de uma entidade de impacto crítico deve ser realizada periodicamente, o mais tardar 36 meses após o termo da primeira verificação e, posteriormente, de três em três anos.
5. Cada entidade de impacto crítico definida em conformidade com o artigo 24.º deve demonstrar a sua conformidade com os controlos referidos no artigo 28.º, n.º 1, alíneas a), b) e c), e com a criação do sistema de gestão da cibersegurança a que se refere a alínea d) do mesmo artigo, comunicando à autoridade competente os resultados da verificação da conformidade.

*Artigo 32.º***Sistema de gestão da cibersegurança**

1. No prazo de 24 meses após ter sido notificada pela autoridade competente de que foi identificada como entidade de impacto elevado ou de impacto crítico em conformidade com o artigo 24.º, n.º 6, cada entidade de impacto elevado e de impacto crítico deve criar um sistema de gestão da cibersegurança e, posteriormente, revê-lo de três em três anos, a fim de:
 - a) Determinar o âmbito do sistema de gestão da cibersegurança tendo em conta as interfaces e as dependências com outras entidades;
 - b) Assegurar que todos os seus quadros superiores são informados das obrigações jurídicas pertinentes e contribuem ativamente para a aplicação do sistema de gestão da cibersegurança mediante decisões atempadas e de reações rápidas;
 - c) Assegurar a disponibilização dos recursos necessários para o sistema de gestão da cibersegurança;
 - d) Estabelecer uma política de cibersegurança que deve ser documentada e comunicada no seio da entidade e às partes afetadas pelos riscos de segurança;
 - e) Atribuir e comunicar as responsabilidades pelas funções pertinentes para a cibersegurança;
 - f) Efetuar a gestão dos riscos de cibersegurança a nível da entidade, tal como definido no artigo 26.º;
 - g) Determinar e disponibilizar os recursos necessários para a aplicação, manutenção e melhoria contínua do sistema de gestão da cibersegurança, tendo em conta a competência necessária e a sensibilização para os recursos de cibersegurança;
 - h) Determinar a comunicação interna e externa pertinente para a cibersegurança;
 - i) Criar, atualizar e controlar informações documentadas relacionadas com o sistema de gestão da cibersegurança;
 - j) Avaliar o desempenho e a eficácia do sistema de gestão da cibersegurança;
 - k) Realizar auditorias internas a intervalos planeados, para assegurar que o sistema de gestão da cibersegurança é efetivamente aplicado e mantido;

- l) Analisar a aplicação do sistema de gestão da cibersegurança a intervalos planeados; controlar e corrigir a não conformidade dos recursos e atividades com as políticas, os procedimentos e as orientações do sistema de gestão da cibersegurança.
2. O âmbito do sistema de gestão da cibersegurança deve incluir todos os ativos no perímetro de impacto elevado e de impacto crítico da entidade de impacto elevado e de impacto crítico.
3. As autoridades competentes devem, sem impor nem discriminar a favor da utilização de um determinado tipo de tecnologia, incentivar a utilização de normas e especificações europeias ou internacionais relacionadas com os sistemas de gestão e que sejam pertinentes para a segurança dos sistemas de rede e informação.

Artigo 33.º

Controlos de cibersegurança mínimos e avançados da cadeia de abastecimento

1. No prazo de sete meses após a apresentação do primeiro projeto de relatório de avaliação dos riscos de cibersegurança à escala da União nos termos do artigo 19.º, n.º 4, os ORT, com o apoio da REORT para a Eletricidade e em cooperação com a entidade ORDUE, devem elaborar uma proposta de controlos de cibersegurança mínimos e avançados da cadeia de abastecimento que atenuem os riscos da cadeia de abastecimento identificados nas avaliações dos riscos de cibersegurança à escala da União, complementando os controlos de cibersegurança mínimos e avançados elaborados nos termos do artigo 29.º. Os controlos de cibersegurança mínimos e avançados da cadeia de abastecimento devem ser elaborados juntamente com os controlos de cibersegurança mínimos e avançados nos termos do artigo 29.º. Os controlos de cibersegurança mínimos e avançados da cadeia de abastecimento devem abranger a totalidade do ciclo de vida de todos os produtos, serviços e processos de TIC nos perímetros de impacto elevado ou de impacto crítico de uma entidade de impacto elevado ou de impacto crítico. O grupo de cooperação SRI deve ser consultado aquando da elaboração da proposta de controlos de cibersegurança mínimos e avançados da cadeia de abastecimento.
2. Os controlos de cibersegurança mínimos da cadeia de abastecimento devem consistir em controlos de entidades de impacto elevado e de impacto crítico que:
 - a) Incluam recomendações para a aquisição de produtos, serviços e processos de TIC referentes a especificações de cibersegurança, abrangendo, pelo menos:
 - i) a verificação dos antecedentes do pessoal do fornecedor que participa na cadeia de abastecimento e que lida com informações sensíveis ou tem acesso aos ativos de impacto elevado ou de impacto crítico da entidade. A verificação dos antecedentes pode incluir uma verificação da identidade e dos antecedentes do pessoal ou dos contratantes de uma entidade, em conformidade com a legislação e os procedimentos nacionais e com o direito pertinente e aplicável da União, incluindo o Regulamento (UE) 2016/679 e a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho⁽¹⁸⁾. As verificações dos antecedentes devem ser proporcionadas e estritamente limitadas ao necessário. Devem ser realizadas exclusivamente para avaliar um possível risco de segurança para a entidade em questão. Devem ser proporcionais aos requisitos comerciais, à classificação das informações às quais se vai aceder e aos riscos percecionados, podendo ser realizadas pela própria entidade, por uma empresa externa que realize uma análise ou por intermédio de uma entidade pública,
 - ii) os processos de conceção, desenvolvimento e produção seguros e controlados de produtos, serviços e processos de TIC, promovendo a conceção e o desenvolvimento de produtos, serviços e processos de TIC que incluam medidas técnicas adequadas para garantir a cibersegurança,
 - iii) a conceção de sistemas de rede e informação nos quais não se confie nos dispositivos, mesmo quando se encontram num perímetro seguro, exijam a verificação de todos os pedidos que recebem e apliquem o princípio do menor privilégio,
 - iv) o acesso do fornecedor aos ativos da entidade,

⁽¹⁸⁾ Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO L 119 de 4.5.2016, p. 89).

- v) as obrigações contratuais do fornecedor de proteger e restringir o acesso às informações sensíveis da entidade,
 - vi) os cadernos de encargos no domínio da cibersegurança subjacentes aos subcontratantes do fornecedor,
 - vii) a rastreabilidade da aplicação das especificações de cibersegurança desde o desenvolvimento, passando pela produção, até à entrega de produtos, serviços ou processos de TIC,
 - viii) o apoio a atualizações de segurança ao longo de todo o ciclo de vida dos produtos, serviços ou processos de TIC,
 - ix) o direito de auditar a cibersegurança nos processos de conceção, desenvolvimento e produção do fornecedor, e
 - x) a avaliação do perfil de risco do fornecedor;
- b) Exijam que essas entidades tenham em conta as recomendações em matéria de contratação referidas na alínea a) aquando da celebração de contratos com fornecedores, parceiros de colaboração e outras partes da cadeia de abastecimento, abrangendo entregas normais de produtos, serviços e processos de TIC, bem como acontecimentos e circunstâncias não solicitados, como a rescisão e a transição de contratos em caso de negligência do parceiro contratual;
- c) Exijam que essas entidades tenham em conta os resultados das avaliações coordenadas pertinentes dos riscos de segurança das cadeias de abastecimento críticas, realizadas em conformidade com o artigo 22.º, n.º 1, da Diretiva (UE) 2022/2555;
- d) Incluam critérios de seleção e contratação de fornecedores que possam cumprir as especificações de cibersegurança referidas na alínea a) e que possuam um nível de cibersegurança adequado aos riscos de cibersegurança do produto, serviço ou processo de TIC que o fornecedor distribui;
- e) Incluam critérios para diversificar as fontes de abastecimento de produtos, serviços e processos de TIC e para reduzir o risco de dependência de um fornecedor;
- f) Incluam critérios para acompanhar, rever ou auditar periodicamente as especificações de cibersegurança dos processos operacionais internos dos fornecedores ao longo de todo o ciclo de vida de cada produto, serviço e processo de TIC.

3. No que respeita às especificações de cibersegurança constantes da recomendação relativa à contratação no domínio da cibersegurança a que se refere o n.º 2, alínea a), as entidades de impacto elevado ou de impacto crítico devem utilizar os princípios da contratação previstos na Diretiva 2014/24/UE do Parlamento Europeu e do Conselho⁽¹⁹⁾, em conformidade com o artigo 35.º, n.º 4, ou definir as suas próprias especificações com base nos resultados da avaliação dos riscos de cibersegurança a nível das entidades.

4. Os controlos de cibersegurança avançados da cadeia de abastecimento devem incluir controlos para que as entidades de impacto crítico verifiquem, durante a contratação, se os produtos, serviços e processos de TIC que serão utilizados como ativos de impacto crítico satisfazem as especificações de cibersegurança. O produto, serviço ou processo de TIC deve ser verificado no âmbito de um sistema europeu de certificação da cibersegurança a que se refere o artigo 31.º ou através de atividades de verificação selecionadas e organizadas pela entidade. A profundidade e a amplitude das atividades de verificação devem ser suficientes para garantir que o produto, serviço ou processo de TIC pode ser utilizado para atenuar os riscos identificados na avaliação dos riscos a nível das entidades. A entidade de impacto crítico deve documentar as medidas tomadas para reduzir os riscos identificados.

5. Os controlos de cibersegurança mínimos e avançados da cadeia de abastecimento são aplicáveis à aquisição de produtos, serviços e processos de TIC pertinentes. Os controlos de cibersegurança mínimos e avançados da cadeia de abastecimento serão aplicáveis aos processos de contratação nas entidades identificadas como entidades de impacto crítico e de impacto elevado nos termos do artigo 24.º, seis meses após a adoção ou atualização dos controlos de cibersegurança mínimos e avançados referidos no artigo 29.º.

⁽¹⁹⁾ Diretiva 2014/24/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa aos contratos públicos e que revoga a Diretiva 2004/18/CE (JO L 94 de 28.3.2014, p. 65).

6. No prazo de seis meses após a elaboração de cada relatório da avaliação regional dos riscos de cibersegurança nos termos do artigo 21.º, n.º 2, os ORT, com o apoio da REORT para a Eletricidade e em cooperação com a entidade ORDUE, devem propor à autoridade competente uma alteração dos controlos de cibersegurança mínimos e avançados da cadeia de abastecimento. A proposta será elaborada em conformidade com o artigo 8.º, n.º 10, e terá em conta os riscos identificados na avaliação regional dos riscos.

Artigo 34.º

Matriz de mapeamento dos controlos de cibersegurança da eletricidade com base em normas

1. No prazo de sete meses após a apresentação do primeiro projeto de relatório de avaliação dos riscos de cibersegurança à escala da União nos termos do artigo 19.º, n.º 4, os ORT, com o apoio da REORT para a Eletricidade, em cooperação com a entidade ORDUE e em consulta com a ENISA, devem elaborar uma proposta de matriz para mapear os controlos previstos no artigo 28.º, n.º 1, alíneas a) e b), com base em normas europeias e internacionais selecionadas, bem como nas especificações técnicas pertinentes («matriz de mapeamento»). A REORT para a Eletricidade e a entidade ORDUE devem documentar a equivalência dos diferentes controlos aos controlos previstos no artigo 28.º, n.º 1, alíneas a) e b).

2. As autoridades competentes podem fornecer à REORT para a Eletricidade e à entidade ORDUE um levantamento dos controlos previstos no artigo 28.º, n.º 1, alíneas a) e b), com uma referência aos quadros legislativos ou regulamentares nacionais conexos, incluindo as normas nacionais pertinentes dos Estados-Membros nos termos do artigo 25.º da Diretiva (UE) 2022/2555. Se a autoridade competente de um Estado-Membro fornecer esse levantamento, a REORT para a Eletricidade e a entidade ORDUE devem integrar esse levantamento nacional na matriz de mapeamento.

3. No prazo de seis meses após a elaboração de cada relatório da avaliação regional dos riscos de cibersegurança nos termos do artigo 21.º, n.º 2, os ORT, com o apoio da REORT para a Eletricidade, em cooperação com a entidade ORDUE e em consulta com a ENISA, devem propor à autoridade competente uma alteração da matriz de mapeamento. A proposta será elaborada em conformidade com o artigo 8.º, n.º 10, e terá em conta os riscos identificados na avaliação regional dos riscos.

CAPÍTULO IV

RECOMENDAÇÕES EM MATÉRIA DE CONTRATAÇÃO NO DOMÍNIO DA CIBERSEGURANÇA

Artigo 35.º

Recomendações em matéria de contratação no domínio da cibersegurança

1. Os ORT, com o apoio da REORT para a Eletricidade e em cooperação com a entidade ORDUE, devem elaborar, num programa de trabalho a estabelecer e a atualizar sempre que seja adotado um relatório da avaliação regional dos riscos de cibersegurança, conjuntos de recomendações não vinculativas em matéria de contratação no domínio da cibersegurança que as entidades de impacto elevado e de impacto crítico possam utilizar como base para a aquisição de produtos, serviços e processos de TIC nos perímetros de impacto elevado e de impacto crítico. Esse programa de trabalho deve incluir os seguintes elementos:

- a) Uma descrição e classificação dos tipos de produtos, serviços e processos de TIC utilizados por entidades de impacto elevado e de impacto crítico nos perímetros de impacto elevado e de impacto crítico;
- b) Uma lista dos tipos de produtos, serviços e processos de TIC para os quais deve ser elaborado um conjunto de recomendações não vinculativas no domínio da cibersegurança com base nos relatórios das avaliações regionais dos riscos de cibersegurança pertinentes e nas prioridades das entidades de impacto elevado e de impacto crítico.

2. A REORT para a Eletricidade, em cooperação com a entidade ORDUE, deve, no prazo de seis meses após a adoção ou atualização do relatório da avaliação regional dos riscos de cibersegurança, apresentar à ACER um resumo desse programa de trabalho.

3. Os ORT, com o apoio da REORT para a Eletricidade e em cooperação com a entidade ORDUE, devem procurar assegurar que as recomendações não vinculativas em matéria de contratação no domínio da cibersegurança elaboradas com base nas avaliações regionais dos riscos de cibersegurança pertinentes sejam semelhantes ou comparáveis em todas as regiões de exploração da rede. Os conjuntos de recomendações em matéria de contratação no domínio da cibersegurança devem abranger, pelo menos, as especificações referidas no artigo 33.º, n.º 2, alínea a). Sempre que possível, as especificações devem ser selecionadas a partir de normas europeias e internacionais.
4. Os ORT, com o apoio da REORT para a Eletricidade e em cooperação com a entidade ORDUE, devem assegurar que os conjuntos de recomendações em matéria de contratação no domínio da cibersegurança:
 - a) Cumprem os princípios da contratação nos termos da Diretiva 2014/24/UE;
 - b) São compatíveis e têm em conta os mais recentes sistemas europeus de certificação da cibersegurança pertinentes para o produto, serviço ou processo de TIC.

Artigo 36.º

Orientações sobre a utilização de sistemas europeus de certificação da cibersegurança para a aquisição de produtos, serviços e processos de TIC

1. As recomendações não vinculativas em matéria de contratação no domínio da cibersegurança elaboradas nos termos do artigo 35.º podem incluir orientações setoriais sobre a utilização de sistemas europeus de certificação da cibersegurança, caso exista um sistema adequado para um tipo de produto, serviço ou processo de TIC utilizado por entidades de impacto crítico, sem prejuízo do enquadramento para a criação de sistemas europeus de certificação da cibersegurança nos termos do artigo 46.º do Regulamento (UE) 2019/881.
2. Os ORT, com o apoio da REORT para a Eletricidade e em cooperação com a entidade ORDUE, devem cooperar estreitamente com a ENISA na disponibilização das orientações setoriais incluídas nas recomendações não vinculativas em matéria de contratação no domínio da cibersegurança nos termos do n.º 1.

CAPÍTULO V

FLUXOS DE INFORMAÇÃO, CIBERATAQUES E GESTÃO DE CRISES

Artigo 37.º

Regras em matéria de partilha de informações

1. Se uma autoridade competente receber informações relacionadas com um ciberataque sujeito a notificação, essa autoridade competente:
 - a) Avalia o nível de confidencialidade dessas informações e informa a entidade sobre o resultado da sua avaliação sem demora injustificada e, o mais tardar, no prazo de 24 horas após a receção das informações;
 - b) Tenta encontrar qualquer ciberataque semelhante na União notificado a outras autoridades competentes, a fim de correlacionar as informações recebidas no contexto do ciberataque sujeito a notificação com as informações disponibilizadas no contexto de outros ciberataques, de suplementar as informações existentes e de reforçar e coordenar as respostas em matéria de cibersegurança;
 - c) É responsável pela supressão dos segredos comerciais e pela anonimização das informações em conformidade com as regras nacionais e da União aplicáveis;

- d) Partilha as informações com os pontos de contacto únicos nacionais, as CSIRT e todas as autoridades competentes designadas nos termos do artigo 4.º noutros Estados-Membros, sem demora injustificada e, o mais tardar, 24 horas após a receção de um ciberataque sujeito a notificação, e disponibiliza periodicamente informações atualizadas a essas autoridades ou organismos;
 - e) Divulga as informações do ciberataque, após anonimização e supressão dos segredos comerciais nos termos do n.º 1, alínea c), às entidades de impacto crítico e de impacto elevado no seu Estado-Membro, sem demora injustificada e, o mais tardar, 24 horas após a receção das informações nos termos do n.º 1, alínea a), e fornece periodicamente informações atualizadas que permitam às entidades organizar eficazmente a sua defesa;
 - f) Pode solicitar à entidade de impacto elevado ou de impacto crítico à qual divulgou as informações que transmita, de forma segura, as informações sobre o ciberataque sujeito a notificação a outras entidades que possam ser afetadas, com o objetivo de gerar um conhecimento da situação por parte do setor da eletricidade e evitar a ocorrência de um risco que possa evoluir para um incidente de cibersegurança transfronteiriço no setor da eletricidade;
 - g) Partilha com a ENISA um relatório de síntese, após anonimização e supressão dos segredos comerciais, com as informações sobre o ciberataque.
2. Se uma CSIRT tomar conhecimento de uma vulnerabilidade ativamente explorada não corrigida, deve:
- a) Partilhá-la sem demora com a ENISA através de um canal seguro de intercâmbio de informações adequado, salvo disposição em contrário noutra legislação da União;
 - b) Ajudar a entidade em causa a receber do fabricante ou do fornecedor uma gestão rápida, coordenada e eficaz da vulnerabilidade ativamente explorada não corrigida ou a beneficiar de medidas de atenuação eficazes e eficientes;
 - c) Partilhar as informações disponíveis com o vendedor e solicitar ao fabricante ou fornecedor, sempre que possível, que identifique uma lista de CSIRT nos Estados-Membros afetados pela vulnerabilidade ativamente explorada não corrigida e que devem ser informadas;
 - d) Partilhar as informações disponíveis com as CSIRT identificadas na alínea anterior, com base no princípio da necessidade de conhecer;
 - e) Partilhar, caso existam, as estratégias e medidas de atenuação da vulnerabilidade ativamente explorada não corrigida comunicada.
3. Se uma autoridade competente tomar conhecimento de uma vulnerabilidade ativamente explorada não corrigida, essa autoridade competente deve:
- a) Partilhar, caso existam, as estratégias e medidas de atenuação da vulnerabilidade ativamente explorada não corrigida comunicada, em coordenação com as CSIRT do seu Estado-Membro;
 - b) Partilhar as informações com uma CSIRT do Estado-Membro no qual foi comunicada a vulnerabilidade ativamente explorada não corrigida.
4. Se a autoridade competente tomar conhecimento de uma vulnerabilidade não corrigida em relação à qual não possui elementos de prova de que está a ser ativamente explorada, deve coordenar-se sem demora injustificada com a CSIRT para efeitos de divulgação coordenada de vulnerabilidades, tal como previsto no artigo 12.º, n.º 1, da Diretiva (UE) 2022/2555.
5. Se uma CSIRT receber informações relacionadas com ciberameaças de uma ou várias entidades de impacto elevado ou de impacto crítico nos termos do artigo 38.º, n.º 6, deve divulgar essas informações ou quaisquer outras informações importantes para prevenir, detetar, responder ou atenuar o risco conexo a entidades de impacto crítico e de impacto elevado no seu Estado-Membro e, se for caso disso, a todas as CSIRT em causa e ao seu ponto de contacto único nacional, sem demora injustificada e, o mais tardar, quatro horas após a receção das informações.
6. Se uma autoridade competente tomar conhecimento de informações relacionadas com ciberameaças provenientes de uma ou várias entidades de impacto elevado ou de impacto crítico, deve transmitir essas informações à CSIRT para efeitos do n.º 5.
7. As autoridades competentes podem delegar, no todo ou em parte, as responsabilidades previstas nos n.ºs 3 e 4, relativamente a uma ou mais entidades de impacto elevado ou de impacto crítico que operem em mais de um Estado-Membro, noutra autoridade competente de um desses Estados-Membros, na sequência de um acordo entre as autoridades competentes em causa.

8. Os ORT, com o apoio da REORT para a Eletricidade e em cooperação com a entidade ORDUE, devem desenvolver uma metodologia de classificação de ciberataques até 13 de junho de 2025. Os ORT, com o apoio da REORT para a Eletricidade e da entidade ORDUE, podem solicitar às autoridades competentes que consultem a ENISA e as suas autoridades competentes responsáveis pela cibersegurança para obterem apoio na elaboração dessa escala de classificação. A metodologia deve prever a classificação da gravidade de um ciberataque de acordo com cinco níveis, sendo os dois níveis mais altos o «elevado» e o «crítico». A classificação deve basear-se na avaliação dos seguintes parâmetros:

- a) O impacto potencial tendo em conta os ativos e perímetros expostos, determinado em conformidade com o artigo 26.º, n.º 4, alínea c);
- b) A gravidade do ciberataque.

9. Até 13 de junho de 2026, a REORT para a Eletricidade, em colaboração com a entidade ORDUE, deve realizar um estudo de viabilidade para avaliar a possibilidade e os custos financeiros necessários da criação de uma ferramenta comum que possibilite a todas as entidades partilhar informações com as autoridades nacionais competentes.

10. O estudo de viabilidade deve abordar a possibilidade de essa ferramenta comum:

- a) Apoiar as entidades de impacto crítico e de impacto elevado com informações pertinentes relacionadas com a segurança para as operações de fluxos transfronteiriços de eletricidade, como a comunicação em tempo quase real de ciberataques, alertas precoces relacionados com questões de cibersegurança e vulnerabilidades não divulgadas em equipamentos utilizados na rede de eletricidade;
- b) Ser mantida num ambiente adequado e altamente fiável;
- c) Permitir a recolha de dados de entidades de impacto crítico e de impacto elevado e facilitar a supressão de informações confidenciais e a anonimização dos dados, bem como a sua rápida divulgação a entidades de impacto crítico e de impacto elevado.

11. A REORT para a Eletricidade, em cooperação com a entidade ORDUE, deve:

- a) Consultar a ENISA e o grupo de cooperação SRI, os pontos de contacto únicos nacionais e os representantes das principais partes interessadas ao avaliar a viabilidade;
- b) Apresentar os resultados do estudo de viabilidade à ACER e ao grupo de cooperação SRI.

12. A REORT para a Eletricidade, em cooperação com a entidade ORDUE, pode analisar e facilitar iniciativas propostas por entidades de impacto crítico e de impacto elevado para avaliar e testar essas ferramentas de partilha de informações.

Artigo 38.º

Papel das entidades de impacto elevado e de impacto crítico no que respeita à partilha de informações

1. Cada entidade de impacto elevado e de impacto crítico deve:

- a) Estabelecer, para todos os ativos no seu perímetro de cibersegurança determinado nos termos do artigo 26.º, n.º 4, alínea c), pelo menos as capacidades do centro de operações de cibersegurança para:
 - i) assegurar que os sistemas e aplicações de rede e informação pertinentes fornecem registos de segurança para o controlo da segurança, a fim de permitir a deteção de anomalias e recolher informações sobre ciberataques,
 - ii) efetuar controlos de segurança, incluindo a deteção de intrusões e a avaliação das vulnerabilidades dos sistemas de rede e informação,
 - iii) analisar e, se for caso disso, tomar todas as medidas necessárias, no âmbito da sua responsabilidade e capacidade, para proteger a entidade,
 - iv) participar na recolha e partilha de informações descritas no presente artigo;
- b) Ter o direito de adquirir a totalidade ou parte dessas capacidades nos termos da alínea a) através de prestadores de serviços de segurança geridos. As entidades de impacto crítico e de impacto elevado continuam a ser responsáveis pelos prestadores de serviços de segurança geridos e supervisionam os seus esforços;

- c) Designar um ponto de contacto único a nível das entidades para efeitos de partilha de informações.
2. A ENISA pode emitir orientações não vinculativas sobre a criação dessas capacidades ou a subcontratação do serviço a prestadores de serviços de segurança geridos, no âmbito da função definida no artigo 6.º, n.º 2, do Regulamento (UE) 2019/881.
3. Cada entidade de impacto crítico e de impacto elevado deve partilhar com as suas CSIRT e a sua autoridade competente as informações pertinentes relacionadas com um ciberataque sujeito a notificação, sem demora injustificada e, o mais tardar, quatro horas após ter tomado conhecimento de que o incidente deve ser sujeito a notificação.
4. As informações relacionadas com um ciberataque devem ser consideradas sujeitas a notificação quando o ciberataque for avaliado pela entidade afetada como tendo um grau de criticalidade que varia entre «elevado» e «crítico», seguindo a metodologia da escala de classificação de ciberataque nos termos do artigo 37.º, n.º 8. O ponto de contacto único a nível das entidades designado nos termos do n.º 1, alínea c), deve comunicar a classificação do incidente.
5. Sempre que as entidades de impacto crítico e de impacto elevado notifiquem informações pertinentes relacionadas com vulnerabilidades ativamente exploradas não corrigidas a uma CSIRT, esta pode transmitir essas informações à sua autoridade competente. Tendo em conta o grau de sensibilidade das informações notificadas, a CSIRT pode reter as informações ou atrasar a sua transmissão com base em motivos justificados relacionados com a cibersegurança.
6. Cada entidade de impacto crítico e de impacto elevado deve disponibilizar às suas CSIRT, sem demora injustificada, quaisquer informações relacionadas com uma ciberameaça sujeita a notificação que possam ter um efeito transfronteiriço. As informações relacionadas com uma ciberameaça devem ser consideradas sujeitas a notificação caso se verifique pelo menos uma das seguintes condições:
- a) Fornecem informações pertinentes a outras entidades de impacto crítico e de impacto elevado para prevenir, detetar, responder ou atenuar o impacto do risco;
- b) As técnicas, táticas e procedimentos identificados utilizados no contexto de um ataque conduzem a informações como endereços URL ou IP comprometidos, valores de dispersão ou qualquer outro atributo útil para contextualizar e correlacionar o ataque;
- c) Uma ciberameaça pode ser avaliada e contextualizada com informações adicionais fornecidas por prestadores de serviços ou por terceiros não abrangidos pelo presente regulamento.
7. Cada entidade de impacto crítico e de impacto elevado deve, ao partilhar informações nos termos do presente artigo, especificar o seguinte:
- a) Que as informações são apresentadas nos termos do presente regulamento;
- b) Se as informações dizem respeito:
- i) a um ciberataque sujeito a notificação a que se refere o n.º 3,
- ii) a vulnerabilidades ativamente exploradas não corrigidas que não sejam do conhecimento público a que se refere o n.º 4,
- iii) a um ciberataque sujeito a notificação a que se refere o n.º 5;
- c) No caso de um ciberataque sujeito a notificação, o nível do ciberataque de acordo com a metodologia da escala de classificação de ciberataques referida no artigo 37.º, n.º 8, e as informações conducentes a essa classificação, incluindo, pelo menos, o carácter crítico do ciberataque.
8. Quando uma entidade de impacto crítico ou de impacto elevado notifica um incidente significativo nos termos do artigo 23.º da Diretiva (UE) 2022/2555 e a notificação de incidentes ao abrigo desse artigo contém informações pertinentes, tal como exigido no n.º 3 do presente artigo, a notificação da entidade nos termos do artigo 23.º, n.º 1, dessa diretiva constitui uma comunicação de informações nos termos do n.º 3 do presente artigo.
9. Cada entidade de impacto crítico e de impacto elevado deve prestar informações à sua autoridade competente ou à sua CSIRT, identificando claramente as informações específicas que só devem ser partilhadas com a autoridade competente ou a CSIRT nos casos em que a partilha de informações possa estar na origem de um ciberataque. Cada entidade de impacto crítico e de impacto elevado tem o direito de fornecer uma versão não confidencial das informações à CSIRT competente.

Artigo 39.º

Deteção de ciberataques e tratamento das informações conexas

1. As entidades de impacto crítico e de impacto elevado devem desenvolver as capacidades necessárias para lidar com os ciberataques detetados, com o apoio necessário da autoridade competente, da REORT para a Eletricidade e da entidade ORDUE. As entidades de impacto crítico e de impacto elevado podem ser apoiadas pela CSIRT designada no respetivo Estado-Membro no âmbito da função atribuída às CSIRT pelo artigo 11.º, n.º 5, alínea a), da Diretiva (UE) 2022/2555. As entidades de impacto crítico e de impacto elevado devem aplicar processos eficazes para identificar, classificar e responder a ciberataques que afetem ou possam afetar os fluxos transfronteiriços de eletricidade, a fim de minimizar o seu impacto.
2. Se um ciberataque tiver um efeito nos fluxos transfronteiriços de eletricidade, os pontos de contacto únicos a nível das entidades de impacto crítico e de impacto elevado afetadas devem cooperar para partilhar informações entre si, coordenados pela autoridade competente do Estado-Membro no qual o ciberataque foi notificado pela primeira vez.
3. As entidades de impacto crítico e de impacto elevado devem:
 - a) Assegurar que o seu próprio ponto de contacto único a nível das entidades tenha acesso, com base no princípio da necessidade de conhecer, às informações que receberam do ponto de contacto único nacional por intermédio da respetiva autoridade competente;
 - b) Salvo se já o tiverem feito nos termos do artigo 3.º, n.º 4, da Diretiva (UE) 2022/2555, comunicar à autoridade competente do Estado-Membro no qual estão estabelecidas e ao ponto de contacto único nacional a lista dos seus pontos de contacto únicos para a cibersegurança a nível das entidades:
 - i) dos quais essa autoridade competente e o ponto de contacto único nacional podem esperar receber informações sobre ciberataques sujeitos a notificação,
 - ii) aos quais as autoridades competentes e os pontos de contacto únicos nacionais podem ter de prestar informações;
 - c) Estabelecer procedimentos de gestão de ciberataques, incluindo funções e responsabilidades, tarefas e reações, com base na evolução observável do ciberataque nos perímetros de impacto crítico e de impacto elevado;
 - d) Testar os procedimentos globais de gestão de ciberataques pelo menos uma vez por ano, testando pelo menos um cenário que afete direta ou indiretamente os fluxos transfronteiriços de eletricidade. Esse teste anual pode ser realizado por entidades de impacto crítico e de impacto elevado durante os exercícios periódicos referidos no artigo 43.º. Qualquer atividade de resposta a ciberataques em direto com uma consequência classificada no mínimo na escala 2, de acordo com a metodologia da escala de classificação de ciberataques referida no artigo 37.º, n.º 8, e com uma causa subjacente relacionada com a cibersegurança pode servir como teste anual do plano de resposta a ciberataques.
4. As funções referidas no n.º 1 podem ser delegadas pelos Estados-Membros nos centros de coordenação regionais, em conformidade com o artigo 37.º, n.º 2, do Regulamento (UE) 2019/943.

Artigo 40.º

Gestão de crises

1. Quando a autoridade competente determinar que uma crise de eletricidade está relacionada com um ciberataque com impacto em mais do que um Estado-Membro, as autoridades competentes dos Estados-Membros afetados, as autoridades competentes responsáveis pela cibersegurança, as autoridades competentes em matéria de preparação para riscos e as autoridades de gestão de cibercrises do sistema de rede e informação dos Estados-Membros afetados devem criar conjuntamente um grupo *ad hoc* de coordenação de crises transfronteiriças.
2. O grupo *ad hoc* de coordenação de crises transfronteiriças deve:
 - a) Coordenar a recolha eficiente e a posterior divulgação de todas as informações pertinentes em matéria de cibersegurança às entidades que intervêm no processo de gestão de crises;

- b) Organizar a comunicação entre todas as entidades afetadas pela crise e as autoridades competentes, a fim de reduzir as sobreposições e aumentar a eficiência das análises e das respostas técnicas para corrigir as crises de eletricidade simultâneas com uma causa subjacente relacionada com a cibersegurança;
 - c) Proporcionar, em cooperação com as CSIRT competentes, os conhecimentos especializados necessários, incluindo aconselhamento operacional sobre a aplicação de eventuais medidas de atenuação, às entidades afetadas pelo incidente;
 - d) Notificar e apresentar periodicamente informações atualizadas sobre o estado do incidente à Comissão e ao Grupo de Coordenação da Eletricidade, de acordo com os princípios de proteção estabelecidos no artigo 46.º;
 - e) Procurar aconselhamento junto das autoridades, agências ou entidades competentes que possam ser úteis para atenuar a crise de eletricidade.
3. Se o ciberataque for considerado ou for suscetível de ser considerado um incidente de cibersegurança em grande escala, o grupo *ad hoc* de coordenação de crises transfronteiriças deve informar imediatamente as autoridades nacionais de gestão de cibersegurança, em conformidade com o artigo 9.º, n.º 1, da Diretiva (UE) 2022/2555, nos Estados-Membros afetados pelo incidente, bem como a Comissão e a UE-CyCLONE. Nesse caso, o grupo *ad hoc* de coordenação de crises transfronteiriças deve apoiar a UE-CyCLONE no que respeita às especificidades setoriais.
4. As entidades de impacto crítico e de impacto elevado devem desenvolver e ter à sua disposição capacidades, orientações internas, planos de preparação e pessoal para participar na deteção e atenuação de crises transfronteiriças. A entidade de impacto crítico ou de impacto elevado afetada por uma crise de eletricidade simultânea deve investigar as causas subjacentes dessa crise, em cooperação com a sua autoridade competente, a fim de determinar em que medida a crise está relacionada com um ciberataque.
5. As funções referidas no n.º 4 podem ser delegadas pelos Estados-Membros nos centros de coordenação regionais, em conformidade com o artigo 37.º, n.º 2, do Regulamento (UE) 2019/943.

Artigo 41.º

Planos de gestão de crises de cibersegurança e de resposta a estas

1. No prazo de 24 meses após a notificação à ACER do relatório de avaliação dos riscos à escala da União, a ACER deve, em estreita cooperação com a ENISA, a REORT para a Eletricidade, a entidade ORDUE, as autoridades competentes responsáveis pela cibersegurança, as autoridades competentes, as autoridades competentes em matéria de preparação para riscos, as ERN e as autoridades nacionais de gestão de cibersegurança do sistema de rede e informação, elaborar um plano de gestão de crises de cibersegurança e de resposta a estas à escala da União para o setor da eletricidade.
2. No prazo de 12 meses após a elaboração pela ACER do plano de gestão de crises de cibersegurança e de resposta a estas à escala da União para o setor da eletricidade nos termos do n.º 1, cada autoridade competente deve elaborar um plano nacional de gestão de crises de cibersegurança e de resposta a estas para os fluxos transfronteiriços de eletricidade, tendo em conta o plano de gestão de crises de cibersegurança à escala da União e o plano nacional de preparação para riscos elaborado em conformidade com o artigo 10.º do Regulamento (UE) 2019/941. Este plano deve ser coerente com o plano de resposta a crises e a incidentes de cibersegurança em grande escala previsto no artigo 9.º, n.º 4, da Diretiva (UE) 2022/2555. A autoridade competente deve coordenar-se com as entidades de impacto crítico e de impacto elevado e com a autoridade competente em matéria de preparação para riscos do seu Estado-Membro.
3. O plano nacional de resposta a crises e a incidentes de cibersegurança em grande escala exigido nos termos do artigo 9.º, n.º 4, da Diretiva (UE) 2022/2555 é considerado um plano nacional de gestão de crises de cibersegurança nos termos do presente artigo se incluir disposições em matéria de gestão e resposta a crises para os fluxos transfronteiriços de eletricidade.
4. As tarefas enumeradas nos n.ºs 1 e 2 podem ser delegadas pelos Estados-Membros nos centros de coordenação regionais, em conformidade com o artigo 37.º, n.º 2, do Regulamento (UE) 2019/943.
5. As entidades de impacto crítico e de impacto elevado devem assegurar que os seus processos de gestão de crises relacionados com a cibersegurança:
- a) Dispõem de procedimentos de tratamento de incidentes de cibersegurança transfronteiriços compatíveis, tal como definidos no artigo 6.º, ponto 8), da Diretiva (UE) 2022/2555, formalmente incorporados nos seus planos de gestão de crises;

b) Fazem parte das atividades gerais de gestão de crises.

6. No prazo de 12 meses após a notificação das entidades de impacto elevado e de impacto crítico nos termos do artigo 24.º, n.º 6, e posteriormente de três em três anos, as entidades de impacto crítico e de impacto elevado devem elaborar um plano de gestão de crises a nível das entidades para uma crise relacionada com a cibersegurança, que deve ser incluído nos seus planos gerais de gestão de crises. Esse plano deve incluir, pelo menos, os seguintes elementos:

a) Regras de declaração de crise, tal como estabelecido no artigo 14.º, n.ºs 2 e 3 do Regulamento (UE) 2019/941;

b) Funções e responsabilidades claras em matéria de gestão de crises, nomeadamente a função de outras entidades de impacto crítico e de impacto elevado pertinentes;

c) Informações de contacto atualizadas, bem como regras para a comunicação e a partilha de informações durante uma situação de crise, incluindo a ligação às CSIRT.

7. As medidas de gestão de crises nos termos do artigo 21.º, n.º 2, alínea c), da Diretiva (UE) 2022/2555 são consideradas um plano de gestão de crises a nível das entidades do setor da eletricidade ao abrigo do presente artigo se incluírem todos os requisitos enumerados no n.º 6.

8. Os planos de gestão de crises devem ser testados durante os exercícios de cibersegurança a que se referem os artigos 43.º, 44.º e 45.º.

9. As entidades de impacto crítico e de impacto elevado devem incluir os seus planos de gestão de crises a nível das entidades nos seus planos de continuidade das atividades para os processos de impacto crítico e de impacto elevado. Os planos de gestão de crises a nível das entidades devem incluir:

a) Os processos dependentes da disponibilidade, integridade e fiabilidade dos serviços informáticos;

b) Todos os locais de continuidade das atividades, incluindo os locais dos programas informáticos ou dos equipamentos informáticos;

c) Todas as funções e responsabilidades internas relacionadas com os processos de continuidade das atividades.

10. As entidades de impacto crítico e de impacto elevado devem atualizar os seus planos de gestão de crises a nível das entidades pelo menos de três em três anos e sempre que necessário.

11. A ACER deve atualizar o plano de gestão de crises de cibersegurança e de resposta a estas à escala da União para o setor da eletricidade elaborado nos termos do n.º 1 pelo menos de três em três anos e sempre que necessário.

12. Cada autoridade competente deve atualizar o plano de gestão de crises de cibersegurança e de resposta a estas para os fluxos transfronteiriços de eletricidade elaborado nos termos do n.º 2 pelo menos de três em três anos e sempre que necessário.

13. As entidades de impacto crítico e de impacto elevado devem testar os seus planos de continuidade das atividades pelo menos uma vez de três em três anos ou após alterações importantes num processo de impacto crítico. O resultado dos testes dos planos de continuidade das atividades deve ser documentado. As entidades de impacto crítico e de impacto elevado podem incluir o teste do seu plano de continuidade das atividades nos exercícios de cibersegurança.

14. As entidades de impacto crítico e de impacto elevado devem atualizar o seu plano de continuidade das atividades sempre que necessário e, pelo menos, uma vez de três em três anos, tendo em conta o resultado do teste.

15. Se um teste identificar deficiências no plano de continuidade das atividades, a entidade de impacto crítico e de impacto elevado deve corrigir essas deficiências no prazo de 180 dias consecutivos após o teste e realizar um novo teste para comprovar a eficácia das medidas corretivas.

16. Se uma entidade de impacto crítico ou de impacto elevado não puder corrigir as deficiências no prazo de 180 dias consecutivos, deve incluir os motivos no relatório a apresentar à respetiva autoridade competente em conformidade com o artigo 27.º.

*Artigo 42.º***Capacidades de alerta precoce em matéria de cibersegurança para o setor da eletricidade**

1. As autoridades competentes devem cooperar com a ENISA para desenvolver capacidades de alerta precoce em matéria de cibersegurança da eletricidade, como parte do apoio aos Estados-Membros nos termos do artigo 6.º, n.º 2, e do artigo 7.º do Regulamento (UE) 2019/881.
2. As capacidades de alerta precoce em matéria de cibersegurança da eletricidade devem possibilitar à ENISA, no exercício das funções enumeradas no artigo 7.º, n.º 7, do Regulamento (UE) 2019/881:
 - a) Recolher informações partilhadas a título voluntário junto:
 - i) das CSIRT e autoridades competentes,
 - ii) das entidades enumeradas no artigo 2.º do presente regulamento,
 - iii) de qualquer outra entidade que pretenda partilhar informações pertinentes numa base voluntária;
 - b) Avaliar e classificar as informações recolhidas;
 - c) Avaliar as informações a que a ENISA tem acesso para identificar as condições de ciber-risco e os indicadores pertinentes para aspetos dos fluxos transfronteiriços de eletricidade;
 - d) Identificar condições e indicadores frequentemente correlacionados com ciberataques no setor da eletricidade;
 - e) Definir se devem ser tomadas outras medidas de análise e prevenção através da avaliação e identificação dos fatores de risco;
 - f) Informar as autoridades competentes sobre os riscos identificados e as ações preventivas recomendadas específicas para as entidades em causa;
 - g) Informar todas as entidades pertinentes enumeradas no artigo 2.º dos resultados das informações avaliadas em conformidade com as alíneas b), c) e d) do presente número;
 - h) Incluir periodicamente as informações pertinentes no relatório de conhecimento da situação, emitido em conformidade com o artigo 7.º, n.º 6, do Regulamento (UE) 2019/881;
 - i) Obter, sempre que possível, dados aplicáveis que indiquem uma potencial violação da segurança ou um ciberataque («indicadores de comprometimento») a partir das informações recolhidas.
3. As CSIRT devem divulgar sem demora as informações recebidas da ENISA às entidades em causa, no âmbito das suas funções definidas no artigo 11.º, n.º 3, alínea b), da Diretiva (UE) 2022/2555.
4. A ACER deve acompanhar a eficácia das capacidades de alerta precoce em matéria de cibersegurança da eletricidade. A ENISA deve prestar apoio à ACER, facultando todas as informações necessárias, nos termos do artigo 6.º, n.º 2, e do artigo 7.º, n.º 1, do Regulamento (UE) 2019/881. A análise desta atividade de acompanhamento faz parte do acompanhamento previsto nos termos do artigo 12.º do presente regulamento.

CAPÍTULO VI

QUADRO DE EXERCÍCIOS DE CIBERSEGURANÇA NO SETOR DA ELETRICIDADE*Artigo 43.º***Exercícios de cibersegurança a nível das entidades e dos Estados-Membros**

1. Até 31 de dezembro do ano seguinte à notificação das entidades de impacto crítico e, posteriormente, de três em três anos, cada entidade de impacto crítico deve realizar um exercício de cibersegurança que inclua um ou mais cenários de ciberataques que afetem direta ou indiretamente os fluxos transfronteiriços de eletricidade e que estejam relacionados com os riscos identificados durante as avaliações dos riscos de cibersegurança a nível dos Estados-Membros e a nível das entidades, em conformidade com os artigos 20.º e 27.º.

2. Em derrogação do n.º 1, a autoridade competente em matéria de preparação para riscos, após consulta da autoridade competente e da autoridade de gestão de cibersegurança pertinente designada ou estabelecida na Diretiva (UE) 2022/2555 nos termos do artigo 9.º, pode decidir organizar um exercício de cibersegurança a nível dos Estados-Membros, tal como descrito no n.º 1, em vez de realizar o exercício de cibersegurança a nível das entidades. Para o efeito, a autoridade competente deve informar:

- a) Todas as entidades de impacto crítico do seu Estado-Membro, a ERN, as CSIRT e a autoridade competente em matéria de preparação para riscos, o mais tardar até 30 de junho do ano que precede o exercício de cibersegurança a nível das entidades;
- b) Cada entidade que participa no exercício de cibersegurança a nível dos Estados-Membros, o mais tardar seis meses antes da realização do exercício.

3. A autoridade competente em matéria de preparação para riscos, com o apoio técnico das suas CSIRT, organiza o exercício de cibersegurança descrito no n.º 2 a nível dos Estados-Membros de forma independente ou no contexto de outro exercício de cibersegurança nesse Estado-Membro. A fim de poder agrupar estes exercícios, a autoridade competente em matéria de preparação para riscos pode adiar por um ano o exercício de cibersegurança a nível dos Estados-Membros a que se refere o n.º 1.

4. Os exercícios de cibersegurança a nível das entidades e a nível dos Estados-Membros devem ser coerentes com os quadros nacionais de gestão de crises de cibersegurança, em conformidade com o artigo 9.º, n.º 4, alínea d), da Diretiva (UE) 2022/2555.

5. Até 31 de dezembro de 2026 e posteriormente de três em três anos, a REORT para a Eletricidade, em cooperação com a entidade ORDUE, deve disponibilizar um modelo de cenário de exercício para a realização dos exercícios de cibersegurança a nível das entidades e a nível dos Estados-Membros a que se refere o n.º 1. Esse modelo deve ter em conta os resultados da mais recente avaliação dos riscos de cibersegurança a nível das entidades e a nível dos Estados-Membros e incluir os principais critérios de êxito. A REORT para a Eletricidade e a entidade ORDUE devem envolver a ACER e a ENISA na elaboração desse modelo.

Artigo 44.º

Exercícios de cibersegurança regionais ou transregionais

1. Até 31 de dezembro de 2029 e posteriormente de três em três anos, em cada região de exploração da rede, a REORT para a Eletricidade, em cooperação com a entidade ORDUE, deve organizar um exercício de cibersegurança regional. As entidades de impacto crítico na região de exploração da rede devem participar no exercício de cibersegurança regional. A REORT para a Eletricidade, em cooperação com a entidade ORDUE, pode organizar, em vez de um exercício de cibersegurança regional, um exercício de cibersegurança transregional em mais do que uma região de exploração da rede no mesmo período. O exercício deve ter em conta outras avaliações e cenários dos riscos de cibersegurança existentes, elaborados a nível da União.

2. A ENISA deve apoiar a REORT para a Eletricidade e a entidade ORDUE na preparação e organização do exercício de cibersegurança a nível regional ou transregional.

3. A REORT para a Eletricidade, em coordenação com a entidade ORDUE, deve informar as entidades de impacto crítico que participem no exercício de cibersegurança regional ou transregional seis meses antes da sua realização.

4. O organizador de um exercício periódico de cibersegurança a nível da União nos termos do artigo 7.º, n.º 5, do Regulamento (UE) 2019/881, ou de qualquer exercício obrigatório de cibersegurança relacionado com o setor da eletricidade no mesmo perímetro geográfico, pode convidar a REORT para a Eletricidade e a entidade ORDUE a participar. Nesses casos, a obrigação prevista no n.º 1 não se aplica, desde que todas as entidades de impacto crítico na região de exploração da rede participem no mesmo exercício.

5. Se a REORT para a Eletricidade e a entidade ORDUE participarem num exercício de cibersegurança a que se refere o n.º 4, podem adiar por um ano o exercício de cibersegurança regional ou transregional referido no n.º 1.

6. Até 31 de dezembro de 2027 e posteriormente de três em três anos, a REORT para a Eletricidade, em coordenação com a entidade ORDUE, deve disponibilizar um modelo de exercício para a realização dos exercícios de cibersegurança regionais e transregionais. Esse modelo deve ter em conta os resultados da mais recente avaliação dos riscos de cibersegurança a nível regional e incluir os principais critérios de êxito. A REORT para a Eletricidade deve consultar a Comissão e pode aconselhar-se junto da ACER, da ENISA e do Centro Comum de Investigação sobre a organização e a execução dos exercícios de cibersegurança regionais e transregionais.

Artigo 45.º

Resultados dos exercícios de cibersegurança a nível das entidades, dos Estados-Membros, regional ou transregional

1. Os prestadores de serviços críticos devem participar nos exercícios de cibersegurança referidos no artigo 43.º, n.ºs 1 e 2, e no artigo 44.º, n.º 1, a pedido de uma entidade de impacto crítico, caso prestem serviços à referida entidade no domínio correspondente ao âmbito do exercício de cibersegurança em causa.
2. Os organizadores dos exercícios de cibersegurança referidos no artigo 43.º, n.ºs 1 e 2, e no artigo 44.º, n.º 1, com o aconselhamento da ENISA, se tal lhe for solicitado, e nos termos do artigo 7.º, n.º 5, do Regulamento (UE) 2019/881, devem analisar e finalizar o exercício de cibersegurança em causa com um relatório que resuma os ensinamentos, dirigido a todos os participantes. O relatório deve incluir:
 - a) Os cenários do exercício, os relatórios das reuniões, as principais posições, os resultados positivos e os ensinamentos retirados em qualquer nível da cadeia de valor da eletricidade;
 - b) Informação sobre se os principais critérios de êxito foram cumpridos;
 - c) Uma lista de recomendações para que as entidades participantes no exercício de cibersegurança pertinente corrijam, adaptem ou alterem os processos e procedimentos relativos a crises de cibersegurança, os modelos de governação associados e quaisquer compromissos contratuais existentes com prestadores de serviços críticos.
3. Se tal for solicitado pela rede de CSIRT, pelo grupo de cooperação SRI ou pela UE-CyCLONE, os organizadores dos exercícios de cibersegurança referidos no artigo 43.º, n.ºs 1 e 2, e no artigo 44.º, n.º 1, devem partilhar os resultados do exercício de cibersegurança em causa. Os organizadores devem partilhar com cada entidade participante nos exercícios as informações referidas no n.º 2, alíneas a) e b), do presente artigo. Os organizadores devem partilhar a lista de recomendações referida no n.º 2, alínea c), do presente artigo exclusivamente com as entidades visadas nas recomendações.
4. Os organizadores dos exercícios de cibersegurança referidos no artigo 43.º, n.ºs 1 e 2, e no artigo 44.º, n.º 1, devem acompanhar periodicamente as entidades que participam nos exercícios no que se refere à aplicação das recomendações nos termos do n.º 2, alínea c), do presente artigo.

CAPÍTULO VII

PROTEÇÃO DAS INFORMAÇÕES

Artigo 46.º

Princípios para a proteção das informações trocadas

1. As entidades enumeradas no artigo 2.º, n.º 1, devem assegurar que as informações fornecidas, recebidas, trocadas ou transmitidas ao abrigo do presente regulamento só são acessíveis com base no princípio da necessidade de conhecer e em conformidade com as regras nacionais e da União aplicáveis em matéria de segurança das informações.
2. As entidades enumeradas no artigo 2.º, n.º 1, devem assegurar que as informações fornecidas, recebidas, trocadas ou transmitidas ao abrigo do presente regulamento são tratadas e monitorizadas durante todo o ciclo de vida dessas informações e que só podem ser divulgadas no final do seu ciclo de vida após serem anonimizadas.

3. As entidades enumeradas no artigo 2.º, n.º 1, devem assegurar a aplicação de todas as medidas de proteção de natureza organizacional e técnica necessárias para salvaguardar e proteger a confidencialidade, a integridade, a disponibilidade e a não rejeição das informações fornecidas, recebidas, trocadas ou transmitidas ao abrigo do presente regulamento, independentemente dos meios utilizados. As medidas de proteção devem:

- a) Ser proporcionadas;
- b) Ter em consideração os riscos de cibersegurança relacionados com ameaças conhecidas, passadas e emergentes a que essas informações possam estar sujeitas no contexto do presente regulamento;
- c) Basear-se em normas e boas práticas nacionais, europeias ou internacionais, na medida do possível;
- d) Ser documentadas.

4. As entidades enumeradas no artigo 2.º, n.º 1, devem assegurar que qualquer pessoa a quem seja concedido acesso às informações fornecidas, recebidas, trocadas ou transmitidas ao abrigo do presente regulamento seja informada sobre as regras de segurança aplicáveis a nível das entidades e sobre as medidas e procedimentos pertinentes para a proteção das informações. Essas entidades devem assegurar que a pessoa em causa reconhece a responsabilidade de proteger as informações de acordo com as instruções dadas durante a sessão de informação.

5. As entidades enumeradas no artigo 2.º, n.º 1, devem assegurar que o acesso às informações fornecidas, recebidas, trocadas ou transmitidas ao abrigo do presente regulamento seja limitado às pessoas:

- a) Que estejam autorizadas a aceder a essas informações com base nas suas funções e restringidas à execução das tarefas atribuídas;
- b) Em relação às quais a entidade pôde avaliar os princípios éticos e de integridade, bem como para as quais não existem provas de resultados negativos de uma verificação de antecedentes para avaliar a fiabilidade da pessoa, em conformidade com as boas práticas e os requisitos normais de segurança da entidade e, se necessário, com as disposições legislativas e regulamentares nacionais.

6. As entidades enumeradas no artigo 2.º, n.º 1, devem obter o acordo escrito da pessoa singular ou coletiva que inicialmente criou ou forneceu as informações, antes de as fornecerem a terceiros não abrangidos pelo âmbito de aplicação do presente regulamento.

7. Uma entidade enumerada no artigo 2.º, n.º 1, pode considerar que estas informações devem ser partilhadas sem cumprir o disposto nos n.ºs 1 e 4 do presente artigo, a fim de evitar uma crise de eletrividade simultânea com uma causa subjacente relacionada com a cibersegurança ou qualquer crise transfronteiriça na União noutro setor. Nesse caso, deve:

- a) Consultar a autoridade competente e ser autorizada por esta a partilhar essas informações;
- b) Anonimizar essas informações sem perder os elementos necessários para informar o público de um risco iminente e grave para os fluxos transfronteiriços de eletrividade e das eventuais medidas de atenuação;
- c) Salvaguardar a identidade do iniciador e das entidades que tenham tratado essas informações ao abrigo do presente regulamento.

8. Em derrogação do n.º 6 do presente artigo, as autoridades competentes podem disponibilizar as informações fornecidas, recebidas, trocadas ou transmitidas ao abrigo do presente regulamento a terceiros não enumerados no artigo 2.º, n.º 1, sem o consentimento prévio por escrito do iniciador das informações, desde que a informem o mais rapidamente possível. Antes de divulgar quaisquer informações fornecidas, recebidas, trocadas ou transmitidas ao abrigo do presente regulamento a um terceiro não enumerado no artigo 2.º, n.º 1, a autoridade competente em causa deve assegurar, de forma razoável, que o terceiro em causa tem conhecimento das regras de segurança em vigor e deve receber garantias razoáveis de que o terceiro em causa consegue proteger as informações recebidas em conformidade com os n.ºs 1 a 5 do presente artigo. A autoridade competente deve anonimizar essas informações sem perder os elementos necessários para informar o público de um risco iminente e grave para os fluxos transfronteiriços de eletricidade e das eventuais medidas de atenuação e salvaguardar a identidade do iniciador das informações. Neste caso, o terceiro não enumerado no artigo 2.º, n.º 1, deve proteger as informações recebidas em conformidade com as disposições já em vigor a nível das entidades ou, se tal não for possível, com as disposições e instruções fornecidas pela autoridade competente pertinente.

9. O presente artigo não se aplica às entidades não enumeradas no artigo 2.º, n.º 1, às quais sejam disponibilizadas informações nos termos do n.º 6 do presente artigo. Neste caso, aplica-se o n.º 7 do presente artigo, ou a autoridade competente pode facultar a essa entidade disposições escritas que deve aplicar nos casos em que as informações sejam recebidas nos termos do presente regulamento.

Artigo 47.º

Confidencialidade das informações

1. As informações fornecidas, recebidas, trocadas ou transmitidas ao abrigo do presente regulamento ficam sujeitas às condições de sigilo profissional estabelecidas nos n.ºs 2 a 5 do presente artigo e aos requisitos estabelecidos no artigo 65.º do Regulamento (UE) 2019/943. As informações fornecidas, recebidas, trocadas ou transmitidas entre as entidades enumeradas no artigo 2.º do presente regulamento, para efeitos de execução deste, devem ser protegidas, tendo em consideração o nível de confidencialidade das informações aplicado pelo iniciador.

2. A obrigação de sigilo profissional é aplicável às entidades enumeradas no artigo 2.º.

3. As autoridades competentes responsáveis pela cibersegurança, as ERN, as autoridades competentes em matéria de preparação para riscos e as CSIRT trocam todas as informações necessárias para o desempenho das suas funções.

4. As informações recebidas, trocadas ou transmitidas entre as entidades enumeradas no artigo 2.º, n.º 1, para efeitos de aplicação do artigo 23.º devem ser anonimizadas e agregadas.

5. As informações recebidas por qualquer entidade ou autoridade sujeita ao presente regulamento no exercício das suas funções não podem ser divulgadas a outra entidade ou autoridade, ressalvados os casos abrangidos pelo direito nacional, pelas demais disposições do presente regulamento ou por outra legislação pertinente da União.

6. Sem prejuízo da legislação nacional ou da União, uma autoridade, entidade ou pessoa singular que receba informações nos termos do presente regulamento não as pode utilizar para outros fins que não o exercício das suas funções ao abrigo do presente regulamento.

7. A ACER, após consulta da ENISA, de todas as autoridades competentes, da REORT para a Eletricidade e da entidade ORDUE, deve, até 13 de Junho de 2025, emitir orientações sobre os mecanismos para o intercâmbio de informações entre todas as entidades enumeradas no artigo 2.º, n.º 1, e, em especial, sobre os fluxos de comunicação previstos, bem como sobre os métodos de anonimização e de agregação de informações para efeitos da aplicação do presente artigo.

8. As informações que forem confidenciais nos termos das regras nacionais e da União só podem ser trocadas com a Comissão e com outras autoridades competentes se tal for necessário para efeitos da aplicação do presente regulamento. As informações trocadas devem limitar-se ao necessário e proporcionado em relação ao objetivo desse intercâmbio. O intercâmbio de informações deve preservar a confidencialidade dessas informações e salvaguardar a segurança e os interesses comerciais das entidades de impacto crítico ou de impacto elevado.

CAPÍTULO VIII

DISPOSIÇÕES FINAIS

Artigo 48.º

Disposições temporárias

1. Até à aprovação dos termos e condições ou metodologias referidos no artigo 6.º, n.º 2, ou dos planos referidos no artigo 6.º, n.º 3, a REORT para a Eletricidade, em cooperação com a entidade ORDUE, deve elaborar orientações não vinculativas sobre as seguintes matérias:
 - a) Um índice provisório de impacto na cibersegurança da eletricidade, nos termos do n.º 2 do presente artigo;
 - b) Uma lista provisória de processos de impacto elevado e de impacto crítico à escala da União, nos termos do n.º 4 do presente artigo;
 - c) Uma lista provisória das normas e controlos europeus e internacionais exigidos pela legislação nacional com relevância para os aspetos de cibersegurança dos fluxos transfronteiriços de eletricidade, nos termos do n.º 6 do presente artigo.
2. Até 13 de outubro de 2024, a REORT para a Eletricidade, em cooperação com a entidade ORDUE, deve elaborar uma recomendação relativa a um índice provisório de impacto na cibersegurança da eletricidade. A REORT para a Eletricidade, em cooperação com a entidade ORDUE, deve notificar às autoridades competentes o índice provisório de impacto na cibersegurança da eletricidade recomendado.
3. Quatro meses após a receção do índice provisório de impacto na cibersegurança da eletricidade recomendado, ou o mais tardar até 13 de fevereiro de 2025, as autoridades competentes identificam os candidatos a entidades de impacto elevado e de impacto crítico no seu Estado-Membro com base no índice de impacto na cibersegurança da eletricidade recomendado e elaboram uma lista provisória de entidades de impacto elevado e de impacto crítico. As entidades de impacto elevado e de impacto crítico identificadas na lista provisória podem cumprir voluntariamente as suas obrigações, tal como estabelecidas no presente regulamento, com base no princípio da precaução. Até 13 de março de 2025, as autoridades competentes devem notificar as entidades identificadas na lista provisória de que foram identificadas como entidades de impacto elevado ou de impacto crítico.
4. Até 13 de dezembro de 2024, a REORT para a Eletricidade, em cooperação com a entidade ORDUE, deve elaborar uma lista provisória de processos de impacto elevado e de impacto crítico à escala da União. As entidades notificadas nos termos do n.º 3 que decidam voluntariamente cumprir as suas obrigações estabelecidas no presente regulamento com base num princípio de precaução devem utilizar a lista provisória de processos de impacto elevado e de impacto crítico para determinar os perímetros provisórios de impacto elevado e de impacto crítico, bem como para determinar quais os ativos a incluir na primeira avaliação dos riscos de cibersegurança a nível das entidades.
5. Até 13 de setembro de 2024, cada autoridade competente nos termos do artigo 4.º, n.º 1, deve fornecer à REORT para a Eletricidade e à entidade ORDUE uma lista da sua legislação nacional pertinente para os aspetos de cibersegurança dos fluxos transfronteiriços de eletricidade.
6. Até 13 de Junho de 2025, a REORT para a Eletricidade, em cooperação com a entidade ORDUE, deve elaborar uma lista provisória das normas e controlos europeus e internacionais exigidos pela legislação nacional pertinentes para os aspetos de cibersegurança dos fluxos transfronteiriços de eletricidade, tendo em conta as informações fornecidas pelas autoridades competentes.
7. A lista provisória de normas e controlos europeus e internacionais deve incluir:
 - a) Normas europeias e internacionais e legislação nacional que forneçam orientações sobre metodologias de gestão dos riscos de cibersegurança a nível das entidades;
 - b) Controlos de cibersegurança equivalentes aos controlos que se espera venham a fazer parte dos controlos de cibersegurança mínimos e avançados.
8. A REORT para a Eletricidade e a entidade ORDUE devem ter em conta os pontos de vista da ENISA e da ACER ao finalizarem a lista provisória de normas. A REORT para a Eletricidade e a entidade ORDUE devem publicar a lista transitória das normas e controlos europeus e internacionais nos seus sítios Web.

9. A REORT para a Eletricidade e a entidade ORDUE devem consultar a ENISA e a ACER sobre as propostas de orientações não vinculativas elaboradas nos termos do n.º 1.
10. Até os controlos de cibersegurança mínimos e avançados serem elaborados nos termos do artigo 29.º e adotados nos termos do artigo 8.º, todas as entidades enumeradas no artigo 2.º, n.º 1, devem esforçar-se por aplicar progressivamente as orientações não vinculativas elaboradas nos termos do n.º 1.

Artigo 49.º

Entrada em vigor

O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em 11 de março de 2024.

Pela Comissão
A Presidente
Ursula VON DER LEYEN