C/2026/5593

6.11.2026

RECOMENDAÇÃO DA COMISSÃO

de 29 de outubro de 2026

relativa a orientações sobre a continuidade operacional e os testes de esforço para os pontos de contacto nacionais no âmbito do Mecanismo de Proteção Civil da União

(C/2026/5593)

A COMISSÃO EUROPEIA,

Tendo em conta a Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho, de 17 de dezembro de 2013, relativa a um Mecanismo de Proteção Civil da União Europeia ([1]), nomeadamente o artigo 7.º,

Considerando o seguinte:

(1) Nos termos do artigo 196.º, n.º 1, alínea b), do Tratado sobre o Funcionamento da União Europeia (TFUE), a União deve promover uma cooperação operacional rápida e eficaz na União entre os serviços nacionais de proteção civil.

(2) A União tem uma competência de apoio no domínio da proteção civil, conforme previsto no artigo 6.º, alínea f), do TFUE.

(3) O Mecanismo de Proteção Civil da União (MPCU), estabelecido na Decisão n.º 1313/2013/UE, visa reforçar a cooperação entre a União e os Estados-Membros e facilitar a coordenação no domínio da proteção civil, a fim de melhorar a eficácia dos sistemas de prevenção, preparação e resposta a catástrofes naturais e de origem humana.

(4) Nos últimos anos, a União assistiu a vários eventos altamente perturbadores, nomeadamente as consequências da pandemia de COVID-19, a guerra de agressão da Rússia contra a Ucrânia, as graves perturbações informáticas em 2024, a tempestade Éowyn, na Irlanda, em janeiro de 2025, e o apagão de 2025 na Península Ibérica. Os eventos de perturbação podem impedir ou atrasar o funcionamento dos sistemas de proteção civil que devem permanecer operacionais 24 horas por dia e 7 dias por semana («24/7»).

(5) O artigo 7.º da Decisão n.º 1313/2013/UE dispõe que o Centro de Coordenação de Resposta de Emergência (CCRE) deve assegurar uma capacidade operacional 24 horas por dia e sete dias por semana ao serviço dos Estados-Membros e da Comissão para prosseguir os objetivos do MPCU. O artigo 3.º da Decisão de Execução (UE) 2025/704 da Comissão ([2]) especifica ainda que cada Estado-Membro deve designar um ponto de contacto nacional (PCN) para o CCRE que esteja disponível 24 horas por dia e sete dias por semana.

(6) A Recomendação da Comissão, de 8 de fevereiro de 2023, sobre os objetivos da União em matéria de resiliência a catástrofes ([3]) insta o CCRE e as autoridades de proteção civil dos Estados-Membros e dos Estados participantes no MPCU, no âmbito dos respetivos mandatos, a reforçarem as suas capacidades de planeamento da continuidade das atividades. Especifica também que o MPCU «deve apoiar a realização de testes de esforço para testar a continuidade das atividades dos centros de operações de emergência e colaborar com os Estados-Membros no seguimento dos ensinamentos retirados e das recomendações». Os testes de esforço dos centros de operações de emergência em toda a Europa serviram de iniciativa emblemática do objetivo n.º 5, intitulado «Garantir um sistema de proteção civil sólido», tal como descrito na Comunicação da Comissão intitulada «Objetivos da União Europeia em matéria de resiliência a catástrofes» ([4]).

([1]) JO L 347 de 20.12.2013, p. 924, ELI: http://data.europa.eu/eli/dec/2013/1313/oj.

([2]) Decisão de Execução (UE) 2025/704 da Comissão, de 10 de abril de 2025, que estabelece as normas de execução da Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho relativa a um Mecanismo de Proteção Civil da União Europeia e que revoga as Decisões de Execução 2014/762/UE e (UE) 2019/1310 da Comissão (JO L, 2025/704, 15.4.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/704/oj).

([3]) JO C 56 de 15.2.2023, p. 1.

([4]) Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões — Objetivos da União Europeia em matéria de resiliência a catástrofes: agir em conjunto para fazer face a futuras situações de emergência, 8.2.2023, COM(2023) 61 final.

(7) Esses esforços estão em consonância com outros quadros que visam reforçar a resiliência, incluindo a Estratégia Europeia para uma União da Preparação ([5]) e os requisitos de base da NATO em matéria de resiliência nacional ([6]). Mais especificamente, a ação n.º 51 da estratégia apela à adoção de «orientações para os "testes de esforço" dos centros de resposta a situações de emergência e de crise em toda a UE».

(8) Nesse contexto, é necessário centrar a atenção na continuidade operacional dos PCN do MPCU e aumentar a sua resiliência, para que possam permanecer operacionais durante eventos de perturbação, reforçando os seus planos e práticas de continuidade operacional através de uma avaliação sistemática e de testes de esforço.

(9) Além disso, as capacidades de resposta que poderiam ser disponibilizadas para intervenção a pedido do MPCU podem não pertencer à autoridade do PCN. Garantir a comunicação com as entidades que gerem essas capacidades durante as perturbações é essencial para a continuidade operacional do MPCU.

(10) As disposições destinadas a assegurar a continuidade podem facilmente passar despercebidas até que ocorra uma perturbação. Essas perturbações não resultam necessariamente de crises ou emergências graves, mas podem resultar de incidentes menores ou de condições negligenciadas ou não ideais. A fim de assegurar uma tomada de decisões informada sobre medidas preventivas e de atenuação, o planeamento da continuidade operacional do PCN exige a identificação de potenciais causas de perturbações que afetem as funções essenciais do PCN ([7]). Além disso, o pessoal que trabalha em turnos 24/7 enfrenta desafios psicossociais e de bem-estar únicos, incluindo problemas de saúde resultantes de turnos noturnos, *stress* relacionado com o trabalho e separação da família. Se não forem resolvidos, estes problemas podem contribuir para o esgotamento profissional, uma elevada rotatividade e uma potencial escassez de pessoal.

(11) Os mecanismos de continuidade operacional deverão permanecer eficazes, independentemente da natureza ou causa da perturbação, quer esta resulte de riscos naturais, acidentes, falhas técnicas, erro humano, falhas nas infraestruturas ou nos serviços públicos essenciais, indisponibilidade de pessoal em grande escala, ações intencionais ou maliciosas, incluindo ciberincidentes e atividades híbridas, ou qualquer outra causa.

(12) Ao se prepararem para potenciais perturbações, os PCN aumentam a sua capacidade de resposta rápida e eficaz, minimizando a duração e o impacto dos eventos de perturbação. Essa preparação não só garante que as operações possam ser retomadas dentro de um prazo aceitável, como também limita as consequências negativas para as partes interessadas e os intervenientes externos que dependem da atividade do PCN, para além de salvaguardar a missão e a reputação da organização.

(13) As perturbações decorrentes de ciberincidentes têm características distintas que merecem especial atenção: ao contrário de outras ameaças à continuidade operacional, podem ser intencionais, propagar-se por sistemas interligados e comprometer a integridade ou a confidencialidade dos dados e das comunicações, e não apenas a sua disponibilidade.

(14) A formação, os exercícios e as atualizações regulares são fundamentais para um programa eficaz de continuidade operacional. Quanto mais frequentemente for praticado um plano de continuidade operacional, mais bem preparada se torna a organização, uma vez que os exercícios ajudam a identificar lacunas e a familiarizar o pessoal com os procedimentos. O pessoal devidamente formado, com uma compreensão clara das suas funções e responsabilidades, tem um desempenho mais eficaz em caso de perturbações. Do mesmo modo, a participação das partes interessadas nos exercícios garante que compreendem os protocolos de comunicação e sabem o que esperar durante eventos de perturbação reais.

(15) Os exercícios, os testes de esforço e os incidentes reais proporcionam ensinamentos valiosos. A fim de assegurar que o plano de continuidade operacional continua a ser válido, este deverá ser regularmente atualizado de modo a incorporar os ensinamentos retirados da formação, dos exercícios, dos testes de esforço, dos eventos reais e dos avanços tecnológicos.

([5]) Comunicação Conjunta ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões — Estratégia para uma União da Preparação, de 26.3.2025, JOIN(2025) 130 final.

([6]) Compromisso de reforçar a resiliência, emitido pelos Chefes de Estado e de Governo que participaram na reunião do Conselho do Atlântico Norte em Varsóvia, em 8 e 9 de julho de 2016.

([7]) Os exemplos incluem atualizações de *software*, alterações não comunicadas do domínio de correio eletrónico institucional, atualizações não comunicadas dos dados de contacto, escassez persistente de pessoal ou a aposentação simultânea de uma grande parte do pessoal essencial, cuja substituição não pode ter início até à data da reforma.

(16) Se o PCN fizer parte de uma entidade abrangida pelas disposições aplicáveis da Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho ([8]), os ensinamentos retirados do teste de esforço deverão ser tidos em conta na aplicação de medidas de gestão dos riscos de cibersegurança, em especial no que diz respeito à continuidade das atividades, à gestão de cópias de segurança, à recuperação de desastres e à gestão de crises.

(17) Assegurar a continuidade operacional da autoridade nacional competente em matéria de proteção civil vai além do funcionamento do seu PCN. Por conseguinte, a presente recomendação pode também servir de referência valiosa para o desenvolvimento da continuidade operacional no âmbito das organizações nacionais e dos sistemas de proteção civil, em conformidade com o considerando 7 da Decisão n.º 1313/2013/UE.

(18) A presente recomendação deverá ser abrangente, refletindo a diversidade das estruturas e funções dos PCN nos Estados-Membros e nos Estados participantes no MPCU. Deverá ser aplicada de forma flexível e adaptada ao mandato, ao contexto, às circunstâncias e ao quadro operacional de cada PCN, dado que cada PCN tem características distintas, funciona num quadro jurídico diferente e enfrenta desafios diferentes, o que pode exigir abordagens adaptadas para assegurar a continuidade operacional.

(19) A presente recomendação baseia-se no resultado das consultas com o grupo de peritos da Comissão sobre continuidade operacional 24/7 em eventos disruptivos, criado pela Comissão em 2025, e deverá complementar as normas e orientações existentes e bem estabelecidas relacionadas com a continuidade das atividades ([9]),

ADOTOU A PRESENTE RECOMENDAÇÃO:

1. DESTINATÁRIOS

As autoridades nacionais competentes dos Estados-Membros e dos Estados participantes no MPCU são as destinatárias da presente recomendação.

Os Estados-Membros podem considerá-la pertinente para outros centros nacionais de crise e entidades gestoras das capacidades do MPCU.

2. DEFINIÇÕES

Para efeitos da presente recomendação, entende-se por:

(a) «**Autoridade nacional competente**», uma autoridade designada por um Estado-Membro ou por um Estado participante no MPCU ([10]) no âmbito do MPCU, tal como referido no artigo 29.º da Decisão 1313/2013/UE;

(b) «**Ponto de contacto nacional» (PCN)**, um ponto de contacto para o CCRE num Estado-Membro ou num Estado participante no MPCU que esteja disponível 24 horas por dia e sete dias por semana, designado em conformidade com o artigo 9.º, n.º 7, da Decisão n.º 1313/2013/UE e com o artigo 3.º, n.º 1, da Decisão de Execução (UE) 2025/704;

(c) «**Funções essenciais**», as atividades, operações ou serviços do PCN que são fundamentais para o cumprimento do seu mandato e missão e que não podem ser interrompidos ou devem ser retomados num prazo curto e predefinido. Para efeitos das presentes orientações, a qualificação de uma função como essencial é determinada pela urgência com que deve ser restabelecida na sequência de uma perturbação, e não apenas pela sua importância estratégica, operacional ou institucional. Por conseguinte, as funções com importância estratégica, operacional ou institucional capazes de resistir a perturbações ou atrasos prolongados sem impacto inaceitável não serão consideradas funções essenciais;

([8]) 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, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([9]) Normas internacionais: ISO 22301:2019 (Sistemas de gestão da continuidade operacional); *Federal Continuity Directive 1* (2017), *Federal Continuity Directive 2* (2017), *Continuity Guidance Circular* (2018, atualização de 2024), *Business Process Analysis and Business Impact Analysis User Guide* (2019) da FEMA; e *Good Practice Guidelines* (2018) do Business Continuity Institute.

([10]) Relativamente aos Estados participantes, ver o artigo 28.º da Decisão n.º 1313/2013/UE.

(d) «**Pessoal essencial**», o pessoal que trabalha no PCN e que desempenha ou apoia funções essenciais, o pessoal que faz parte da equipa responsável pela gestão ou resposta a um evento de perturbação ou que desempenha ambas as funções;

(e) «**Pessoal essencial escasso**», o pessoal essencial cujo número reduzido crie, em caso de ausência ou indisponibilidade para trabalhar, uma vulnerabilidade em termos de continuidade operacional, por possuir as certificações, a credenciação de segurança, a autoridade, a responsabilidade pela tomada de decisões, os direitos de acesso, os conhecimentos, as competências especializadas ou as competências linguísticas necessárias para realizar atividades específicas necessárias para assegurar a continuidade de uma função essencial;

(f) «**Estrangulamento por falta de pessoal**», uma situação em que a continuidade de uma função essencial depende da disponibilidade de um ou mais membros do pessoal essencial escasso;

(g) «**Continuidade operacional**», a capacidade de um PCN para manter as suas funções essenciais — incluindo atividades, operações ou serviços — quando os recursos necessários para essas funções, tais como pessoal essencial, informações recebidas, serviços, produtos, fornecimentos, disposições orçamentais, equipamento, sistemas de tecnologias da informação e comunicação (TIC) ou requisitos de localização, ficam indisponíveis, danificados, inutilizáveis ou são interrompidos;

(h) «**Plano de continuidade operacional**» ou «**plano**», um documento único ou um conjunto de procedimentos de continuidade operacional do PCN;

(i) «**Evento de perturbação**», um incidente ou circunstância que impede ou atrasa substancialmente a execução de uma função essencial do PCN;

(j) «**Recuperação**», o restabelecimento das capacidades operacionais, das instalações, sistemas e recursos do PCN após uma perturbação.

3. RECOMENDAÇÕES PARA A CONTINUIDADE OPERACIONAL DOS PCN

3.1. Principais recomendações

1. O PCN deverá elaborar um plano de continuidade operacional coerente e abrangente ou um conjunto documentado de procedimentos que abranja todos os elementos da continuidade operacional. A secção 3.2 contém recomendações adicionais sobre o plano de continuidade operacional.

2. O objetivo do planeamento da continuidade operacional é assegurar que o PCN possa desempenhar as suas funções essenciais em condições degradadas quando ocorrem eventos de perturbação. Como tal, o planeamento da continuidade operacional deverá partir do princípio de que ocorrerão eventos de perturbação e que as condições normais de funcionamento podem não ser restabelecidas imediatamente ou, em alguns casos, podem não ser restabelecidas de todo. O PCN deverá ser capaz de manter as funções essenciais em condições degradadas, utilizando procedimentos alternativos, instalações alternativas, canais de comunicação alternativos e recursos reduzidos até que seja restabelecida a plena capacidade.

3. Durante os eventos de perturbação, deverá ser dada prioridade aos recursos destinados a apoiar as funções essenciais do PCN. Tal pode implicar que as funções não essenciais possam não ser mantidas.

4. Os mecanismos de continuidade operacional deverão assegurar a recolha, análise, validação e divulgação ininterruptas das informações operacionais necessárias para manter o conhecimento da situação do PCN e apoiar a tomada de decisões durante a perturbação.

5. O pessoal formado é o principal recurso para assegurar a continuidade operacional. Embora o plano de continuidade operacional, as disposições associadas e as medidas de salvaguarda apoiem a continuidade, esta depende, em última análise, da capacidade do pessoal para tomar decisões e aplicar estas medidas sob pressão.

6. O planeamento da continuidade operacional deverá basear-se numa compreensão aprofundada das disposições administrativas e operacionais da organização a que o PCN pertence. Para o efeito, a colaboração entre departamentos deverá ser ativamente promovida e facilitada.

7. O PCN deverá avaliar as potenciais fontes de perturbações das suas atividades. A avaliação deverá centrar-se no seu potencial de perturbação das atividades do PCN e no desenvolvimento de um plano de resposta para assegurar a continuidade das funções essenciais.

8. Ao avaliar as ameaças à continuidade operacional, há que dar especial atenção aos processos sensíveis ao fator tempo e aos pontos de estrangulamento, incluindo:

   (a) Fontes únicas de informação ou informações conhecidas apenas por um grupo limitado de pessoas, incluindo informações classificadas;

   (b) Equipamentos únicos ou prestadores de serviços únicos dos quais dependem funções essenciais;

   (c) Canais de comunicação, pessoas de contacto ou decisores únicos;

   (d) disponibilidade de pessoal essencial escasso.

9. Importa identificar e eliminar os estrangulamentos por falta de pessoal e a nível das instalações, das comunicações, dos sistemas de TIC, da logística e da tomada de decisões. Sempre que inevitável, deverão ser estabelecidas e testadas medidas de prevenção e atenuação adequadas, incluindo as sugeridas na secção 3.9.

10. Todas as perturbações, exercícios e testes de esforço deverão permitir identificar ensinamentos e conduzir a melhorias nos mecanismos de continuidade operacional, reforçando a resiliência ao longo do tempo.

11. Para efeitos da continuidade operacional e dos testes de esforço dos PCN no âmbito do MPCU, há que considerar as seguintes categorias não exaustivas de eventos de perturbação. O anexo I apresenta uma descrição de cada categoria.

   (a) Indisponibilidade das instalações;

   (b) Rutura do fornecimento de eletricidade;

   (c) Perturbação ou falha dos sistemas de TIC;

   (d) Faltas de pessoal em grande escala ou faltas de pessoal essencial escasso.

12. O PCN deverá assegurar a sua capacidade para continuar a operar na eventualidade de ocorrerem um ou mais dos fatores de desencadeamento de continuidade enumerados no ponto 11 *supra*.

3.2. **Plano de continuidade operacional do PCN**

13. Cada PCN deverá elaborar por escrito um plano de continuidade operacional coerente e abrangente, ou um conjunto equivalente de procedimentos documentados, que abranja todos os elementos da continuidade operacional e integre e sistematize a resposta a perturbações, incluindo medidas de atenuação e acordos para uma intervenção imediata.

14. O plano de continuidade operacional deverá prever mecanismos alternativos para todos os processos essenciais, especialmente os que são sensíveis ao fator tempo, assegurando que possam prosseguir em caso de falha dos recursos primários. Os mecanismos de salvaguarda e alternativos deverão ser totalmente independentes. Não deverão depender dos mesmos recursos, como o mesmo edifício, fonte de energia, via de comunicação, plataforma de TIC ou prestador de serviços. Também não deverão criar novas dependências que possam introduzir riscos de perturbação adicionais.

15. O plano de continuidade operacional deverá ser testado regularmente em condições realistas. Os planos que não tenham sido validados através de formação, exercícios ou testes de esforço não deverão ser considerados operacionais. O programa de continuidade operacional deverá incluir formação regular obrigatória para o pessoal essencial; testes e exercícios regulares que envolvam a ativação do plano e a sua revisão e atualização sistemática, assegurando que todo o pessoal e partes interessadas em causa tenham conhecimento das atualizações e recebam formação sobre as mesmas.

16. Consoante a estrutura da organização, o PCN deverá envolver na elaboração do plano de continuidade operacional pessoal que, embora não esteja diretamente envolvido nas funções essenciais, possua a experiência ou os conhecimentos necessários para contribuir para uma compreensão global das funções da organização.

17. Os PCN deverão ponderar a possibilidade de designar, dentro da sua organização, uma função de coordenação da continuidade dedicada ao plano de continuidade operacional. Consoante a dimensão e a estrutura do PCN, a função de coordenação da continuidade deverá ser exercida por um único coordenador, por uma equipa específica que reúna representantes das áreas operacionais relevantes, ou através de outras modalidades adaptadas ao contexto nacional. Sempre que seja constituído um grupo, este deverá incluir membros com conhecimentos especializados nos domínios operacionais relevantes para a execução do plano, como sistemas de TIC, instalações alternativas, recursos humanos ou logística. O papel da função de coordenação da continuidade será assegurar a aplicação coerente, a revisão periódica e a atualização do plano de continuidade operacional, incluindo a verificação dos recursos e disposições em que o plano se baseia.

3.3. **Identificação das funções essenciais**

18. O PCN deverá identificar as suas funções essenciais e criar e manter um inventário das mesmas. Para além das funções relacionadas com o MPCU, como a gestão dos pedidos de assistência e a disponibilização e mobilização de capacidades de resposta do MPCU, o PCN poderá também ter de assegurar a continuidade de outras funções essenciais para a organização. Os exemplos incluem a coordenação com as autoridades nacionais ou regionais, a ligação com outras organizações internacionais, a emissão de alertas ao público e o apoio à tomada de decisões a nível superior.

Para cada função essencial, o PCN deverá estabelecer objetivos de desempenho operacional que definam a degradação máxima aceitável dos serviços durante os eventos de perturbação. Esses objetivos deverão incluir, se for caso disso, o período máximo tolerável de perturbação, os objetivos em matéria de tempo de recuperação, a perda aceitável de informações operacionais, os níveis mínimos de pessoal, a disponibilidade das comunicações e a capacidade de tomada de decisões. Os objetivos deverão orientar a conceção do plano de continuidade operacional e constituir a base para a avaliação do desempenho dos testes de esforço. O anexo II apresenta exemplos de objetivos de desempenho operacional.

19. É aconselhável classificar as funções essenciais de acordo com a sua prioridade ou a urgência com que devem ser retomadas.

3.4. **Análise dos processos operacionais e dos recursos em reserva**

20. Com base no inventário das funções essenciais, o PCN deverá realizar uma análise dos processos operacionais (APO) e desenvolver soluções de salvaguarda para garantir a continuidade das suas funções essenciais. A APO deverá incluir uma compreensão abrangente do modo como as funções operam, determinando, para cada função:

(a) As tarefas que a compõem;

(b) O calendário e a sequência das tarefas, incluindo a duração e as etapas sensíveis ao fator tempo;

(c) Quem executa cada tarefa, incluindo o perfil, os conhecimentos especializados ou a formação necessários;

(d) O fluxo de informações, incluindo a forma como os dados, os pedidos e os resultados circulam entre os intervenientes e os sistemas;

(e) Quem valida ou autoriza o(s) processo(s);

(f) Que recursos são utilizados e que contributos de intervenientes externos são necessários, incluindo informações, conjuntos de dados, serviços, produtos, fornecimentos, disposições orçamentais, equipamento, sistemas de TIC e requisitos de localização, como empresas privadas que fornecem energia ou prestam serviços de segurança. Deverá ser dada especial atenção ao nível de classificação das informações, bem como aos espaços e aos dispositivos utilizados para as gerir;

(g) Que resultados decorrem da função, incluindo informações, produtos ou serviços específicos, ou ações de coordenação, validação ou autorização;

(h) A(s) organização(ões) externa(s) ou os grupos de partes interessadas que recebem o(s) resultado(s);

(i) Que dependências e interdependências existentes são essenciais para as operações, incluindo relações e acordos com intervenientes externos — autoridades de outros Estados-Membros e de Estados participantes no MPCU, parceiros da proteção civil, operadores de infraestruturas essenciais, prestadores de serviços, fornecedores, etc. — especificando os contributos ou resultados esperados;

(j) Que recursos em reserva e mecanismos alternativos estão disponíveis.

21. Ao realizarem a sua análise dos processos operacionais, os PCN são convidados a ter em conta o quadro constante do anexo III.

3.5. **Práticas recomendadas para instalações e equipamentos alternativos**

22. O PCN deverá assegurar a sua capacidade de continuar a funcionar se as suas instalações ficarem temporariamente inacessíveis ou inutilizáveis, nomeadamente assegurando a disponibilidade de equipamentos essenciais.

23. As instalações principais e alternativas, bem como as soluções temporárias, deverão ser seguras e ter um nível de classificação adequado. Tal deverá ser proporcional à natureza das crises em questão e à sensibilidade ou classificação das informações tratadas.

3.6. **Práticas recomendadas para o fornecimento de eletricidade**

24. O PCN deverá assegurar a sua capacidade de continuar a funcionar em caso de cortes de energia localizados ou de apagões generalizados.

25. As instalações principais e alternativas, incluindo instalações temporárias, deverão dispor de sistemas de fornecimento de eletricidade resilientes e de sistemas de reserva, para que o PCN possa continuar a funcionar e a desempenhar as suas funções essenciais durante cortes de energia de longa duração.

26. As medidas previstas para os PCN deverão ser aplicadas, se for caso disso, de forma coerente com os planos nacionais de preparação para riscos no setor da eletricidade estabelecidos ao abrigo do Regulamento (UE) 2019/941 do Parlamento Europeu e do Conselho ([11]) e com os planos preventivos de ação e planos de emergência nacionais estabelecidos ao abrigo do Regulamento (UE) 2017/1938 do Parlamento Europeu e do Conselho ([12]) relativo à segurança do aprovisionamento de gás, bem como com as disposições nacionais em vigor em matéria de gestão de crises.

3.7. **Práticas recomendadas para os sistemas de TIC**

27. O PCN deverá assegurar que os sistemas de TIC que apoiam as suas funções essenciais sejam fiáveis e resilientes. Importa dar especial atenção aos seguintes aspetos:

(a) Continuidade do acesso a bases de dados, documentos e mensagens de correio eletrónico, incluindo a disponibilidade de listas de contactos atualizadas, continuidade da comunicação com o CCRE e com os Estados-Membros e os Estados participantes no MPCU, e continuidade dos sistemas de tratamento e gestão para a recolha e monitorização de informações, bem como para o registo das medidas tomadas;

(b) Integração tecnológica, assegurando a compatibilidade e a interoperabilidade de sistemas essenciais com configurações remotas e locais alternativos, incluindo a capacidade desses locais de se ligarem ao Sistema Comum de Comunicação e de Informação de Emergência (CECIS) e de tratarem informações classificadas quando operam à distância; tais disposições deverão ser verificadas através de testes adequados;

(c) Segurança da informação e das comunicações, incluindo a possibilidade de estabelecer ligações classificadas e de proceder ao intercâmbio de comunicações classificadas, tanto a nível nacional como internacional;

(d) Registos de todos os fornecedores terceiros dos dispositivos e do *software* utilizados no PCN.

([11]) 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, ELI: http://data.europa.eu/eli/reg/2019/941/oj).

([12]) Regulamento (UE) 2017/1938 do Parlamento Europeu e do Conselho, de 25 de outubro de 2017, relativo a medidas destinadas a garantir a segurança do aprovisionamento de gás e que revoga o Regulamento (UE) n.º 994/2010 (JO L 280 de 28.10.2017, p. 1, ELI: http://data.europa.eu/eli/reg/2017/1938/oj).

28. Há que dar especial atenção aos ciberincidentes enquanto categoria distinta de perturbação das TIC. O PCN deverá ponderar o estabelecimento de protocolos de coordenação com a autoridade nacional de cibersegurança, no âmbito dos seus mecanismos de continuidade operacional mais amplos. Essas medidas deverão incluir canais de alerta precoce, protocolos conjuntos de resposta a incidentes e a clarificação das funções durante um ciberincidente que afete o PCN.

3.8. **Práticas recomendadas para os recursos humanos**

29. O PCN deverá assegurar que dispõe de pessoal suficiente para se manter operacional em situações de disponibilidade reduzida de pessoal e que os seus colaboradores possuem os perfis e competências necessárias.

30. O PCN deverá equacionar o seguinte:

(a) Assegurar a disponibilidade de pessoal com as competências e a formação adequadas, incluindo a experiência em matéria de gestão de crises e, se for caso disso, a credenciação de segurança necessária para tratar informações classificadas. Deverá desenvolver e aplicar mecanismos de verificação das competências profissionais e prever programas abrangentes de integração e de formação contínua para manter e reforçar as competências do pessoal, assegurando que este esteja plenamente preparado para responder eficazmente às ativações do MPCU. A formação deverá também abranger a prevenção de perturbações causadas por erros humanos ou por ações maliciosas, incluindo a sensibilização essencial para a cibersegurança e a segurança da informação, como o risco da engenharia social;

(b) Ministrar formação regular para manter o pessoal informado sobre os mecanismos de continuidade operacional e sobre a utilização de equipamentos e sistemas de TIC nos locais principais e alternativos. Deverá explorar a possibilidade de formação adicional para o seu pessoal na gestão de catástrofes e crises de longa duração e nas operações do MPCU;

(c) Elaborar planos para assegurar a rotação do pessoal durante emergências prolongadas, incluindo a gestão da capacidade de intervenção rápida. Deverá criar grupos de trabalho com funções claramente definidas e planos de sucessão para melhorar a coordenação durante crises;

(d) Estabelecer disposições relativas ao transporte de modo a assegurar que, quando necessário, o pessoal essencial possa chegar ao local onde é chamado a desempenhar as suas funções, quer seja no local principal, num local alternativo ou numa unidade móvel;

(e) Estabelecer salvaguardas adequadas para assegurar a proteção da saúde e da segurança do pessoal;

(f) Elaborar planos de bem-estar do pessoal que abranjam alimentação, água, alojamento, acesso às instalações do PCN e apoio psicológico para ajudar o pessoal a lidar com o *stress* e a fadiga. Esses planos deverão prever operações prolongadas em ambientes confinados e ter em conta as circunstâncias individuais ou pessoais do pessoal essencial, incluindo eventuais necessidades relacionadas com a família;

(g) Estabelecer políticas de proteção de dados e de privacidade para assegurar que o planeamento da continuidade respeita a proteção dos dados pessoais durante e após os incidentes.

31. De forma a evitar estrangulamentos por falta de pessoal, as funções essenciais deverão estar apoiadas em mecanismos de continuidade operacional adequados, em formação cruzada estruturada e sistemática e em exercícios regulares, para que possam ser asseguradas por vários membros do pessoal com formação. Nenhuma função essencial deverá depender exclusivamente da disponibilidade de um único membro do pessoal.

3.9. **Medidas de prevenção e atenuação para cada categoria de eventos de perturbação**

32. A secção seguinte apresenta uma lista indicativa de medidas de prevenção e atenuação recomendadas para cada categoria de eventos de perturbação. Embora estas medidas possam ser aplicadas em paralelo, cada Estado-Membro deverá selecionar as opções mais adequadas e eficazes com base no mandato do seu PCN, no contexto, nas circunstâncias, na capacidade, na estrutura do seu quadro operacional e jurídico e nas potenciais causas de perturbações que possam afetar as funções essenciais do seu PCN. A lista não se destina a ser aplicada na íntegra e simultaneamente, uma vez que, em alguns casos, a execução de uma medida pode entrar em conflito com a aplicação de outra ou exigir um investimento excessivo.

33. Medidas de prevenção e atenuação recomendadas para fazer face à indisponibilidade das instalações:

(a) Distribuição geográfica do PCN por dois ou mais centros geograficamente separados que funcionem em simultâneo, assegurando o apoio mútuo e salvaguarda em caso de carga excessiva de trabalho;

(b) Relocalização para instalações alternativas geridas pela autoridade do PCN;

(c) Transporte previamente organizado para o pessoal essencial até às instalações alternativas (nomeadamente em condições meteorológicas adversas);

(d) Trabalho à distância (que implica flexibilidade nas tarefas que podem ser realizadas fora do local físico do PCN);

(e) Unidades móveis de comando e controlo que possam acolher temporariamente o pessoal essencial do PCN;

(f) Ativação de acordos administrativos com outras autoridades para utilização das suas instalações;

(g) Descentralização de poderes.

34. Medidas de prevenção e atenuação recomendadas para fazer face a ruturas do fornecimento de eletricidade:

(a) Ativação de geradores e de unidades de alimentação ininterrupta (UPS);

(b) Acordos e contratos de fornecimento prioritário de combustível com fornecedores;

(c) Autonomia energética e fontes de energia alternativas para funções essenciais;

(d) Maximização da capacidade de energia disponível;

(e) Relocalização para instalações alternativas geridas pela autoridade do PCN com fornecimento de eletricidade garantido;

(f) Trabalho à distância a partir de um edifício com fornecimento de eletricidade garantido;

(g) Unidades móveis de comando e controlo autossuficientes em termos de eletricidade;

(h) Ativação de acordos administrativos com outras autoridades para utilização das suas instalações com fornecimento de eletricidade garantido;

(i) Descentralização de poderes.

35. Medidas de prevenção e atenuação recomendadas para fazer face a perturbações ou falhas dos sistemas de TIC:

(a) Redundância;

(b) Cópias de segurança de dados regulares e seguras, incluindo cópias fora do local e fora de linha;

(c) Sistemas de TIC, plataformas e canais de comunicação alternativos;

(d) Equipas de apoio de TIC de emergência ou unidades técnicas de resposta permanente;

(e) Procedimentos de resposta a ciberincidentes coordenados com a autoridade nacional de cibersegurança;

(f) Cópias fora de linha das listas de contactos essenciais, dos principais procedimentos e dos documentos operacionais;

(g) Unidades móveis de comando e controlo com acesso aos sistemas de TIC principais e de reserva;

(h) Relocalização para instalações alternativas geridas pela autoridade do PCN com acesso aos sistemas de TIC principais e de reserva;

(i) Ativação de acordos administrativos com outras autoridades para utilização das suas instalações com acesso aos sistemas de TIC.

36. Medidas de prevenção e atenuação recomendadas para fazer face a faltas de pessoal em grande escala e faltas de pessoal essencial escasso:

(a) Gestão das horas extraordinárias (solução a curto prazo);

(b) Reafetação de tarefas ao pessoal disponível;

(c) Uma reserva pré-identificada de pessoal formado dentro da instituição, disponível num curto espaço de tempo;

(d) Priorização do recrutamento de pessoal;

(e) Investimento na retenção de pessoal essencial;

(f) Apoio às famílias do pessoal essencial;

(g) Prevenção de estrangulamentos por falta de pessoal através da delegação de competências e da promoção da liderança partilhada.

37. O anexo IV fornece orientações técnicas para a aplicação de cada uma das medidas enumeradas.

3.10. **Continuidade das operações em caso de ativações do MPCU**

38. A fim de reforçar as operações do MPCU e assegurar a continuidade, são recomendadas as seguintes ações:

(a) Se o país tiver acesso aos Serviços Transeuropeus de Telemática entre as Administrações (TESTA) ou ao TESTA-EIRIS (sucessor do TESTA), identificar o coordenador nacional TESTA desse país. Assegurar que o ponto de contacto CECIS do país dispõe dos dados de contacto do coordenador nacional TESTA desse país e que esses dados permanecem atualizados. Assegurar que o ponto de contacto CECIS do país compreende o plano de continuidade operacional do seu acesso local/nacional ao portal TESTA a nível nacional;

(b) Desenvolver protocolos para distinguir entre falhas na conectividade TESTA e falhas na plataforma CECIS ao solicitar assistência através do MPCU, e para permitir pedidos de assistência em caso de perturbação TESTA no país do PCN;

(c) Se for caso disso, explorar acordos de apoio operacional mútuo com outras autoridades nacionais, a fim de assegurar que o PCN possa continuar a desempenhar as suas funções essenciais se uma perturbação degradar significativamente a sua capacidade de continuidade operacional. Em especial, esses acordos deverão envolver as autoridades com acesso à rede TESTA, para que o PCN possa aceder ao CECIS a partir de instalações alternativas;

(d) Se for caso disso, explorar a possibilidade de estabelecer acordos administrativos bilaterais de apoio operacional mútuo com países vizinhos que sejam Estados-Membros ou Estados participantes no MPCU, em situações em que uma perturbação degrade significativamente a capacidade de continuidade operacional do PCN e em que os acordos referidos na alínea b) não sejam viáveis. Esses acordos deverão permitir que o PCN utilize as instalações desses países e aceda à rede TESTA;

(e) Ministrar formação sobre o CECIS aos novos membros do pessoal e agendar exercícios regulares para o pessoal;

(f) Com base na estrutura nacional de proteção civil, o plano de continuidade deverá incluir disposições para assegurar comunicações sem descontinuidades entre o PCN e outras autoridades competentes que, se necessário, estejam autorizadas a solicitar a ativação do MPCU;

(g) O plano de continuidade operacional deverá ter em conta as partes interessadas nacionais que detêm e gerem recursos do MPCU que não pertencem à autoridade do PCN, mas que podem ser disponibilizados para intervenção, mediante pedido, através do MPCU.

39. O plano de continuidade operacional deverá estar alinhado com a Recomendação da Comissão, de 29 de novembro de 2024, sobre as Orientações da UE em matéria de apoio do país anfitrião ([13]), especificamente no que diz respeito às ativações do MPCU pelo PCN e ao seu papel no apoio do país anfitrião ([14]).

([13]) C(2024) 8339.

([14]) O apoio do país anfitrião é definido no artigo 4.º, ponto 9, da Decisão n.º 1313/2013/UE como qualquer ação realizada nas fases de preparação e resposta pelo país que recebe ou presta a assistência, ou pela Comissão, a fim de eliminar obstáculos previsíveis à assistência internacional oferecida por intermédio do Mecanismo da União, incluindo o apoio prestado pelos Estados-Membros para facilitar o trânsito dos meios de assistência pelos seus territórios.

3.11. **Ativação do plano de continuidade operacional**

40. Em função da natureza e da escala da perturbação, o plano de continuidade operacional do PCN deverá definir diferentes níveis de ativação, incluindo uma ativação parcial, em que o PCN continua a operar a partir das suas instalações principais com procedimentos adaptados, e uma ativação plena, que exige a relocalização para instalações alternativas ou outros mecanismos alternativos.

41. Os critérios, os níveis de ativação e os fatores de desencadeamento, bem como a autoridade habilitada a autorizar a ativação, deverão ser definidos a nível nacional, em consonância com a estrutura e o quadro operacional de cada PCN. O anexo V apresenta um exemplo ilustrativo de um fluxo de ativação.

42. Os procedimentos de ativação deverão permitir a ativação atempada de mecanismos de continuidade em resposta a perturbações, quer sejam reais ou previstas, incluindo eventos que ocorram fora do horário normal de trabalho e eventos para os quais exista um aviso prévio.

43. Caso um evento perturbe a continuidade operacional do PCN, desencadeando a ativação do seu plano de continuidade operacional, o PCN deverá ponderar notificar o CCRE.

3.12. **Formação, exercícios e testes regulares**

44. Os planos de continuidade operacional deverão ser regularmente objeto de formação, exercícios e testes. Recomenda-se programar regularmente sessões de sensibilização e informação, bem como sessões de formação e exercícios relacionados com os planos de continuidade. Outras formações regulares, como a formação de integração de novos membros do pessoal, deverão também incorporar os elementos necessários do plano de continuidade operacional. Também deverá ser ponderada a participação de partes interessadas externas que possam ser afetadas por uma perturbação das atividades do PCN em sessões regulares de sensibilização e informação específicas, bem como em exercícios.

45. O plano de continuidade operacional deverá ser testado, no mínimo, anualmente. Deverá equacionar-se a realização de testes mais frequentes sempre que a estrutura, o contexto operacional ou o perfil de risco do PCN o justifiquem.

3.13. **Recuperação**

46. Uma vez atenuados os efeitos negativos do evento de perturbação, o PCN deverá considerar o regresso gradual às operações normais como uma fase distinta da continuidade operacional: a recuperação é a fase em que o PCN transita dos mecanismos de continuidade operacional para as operações normais, incluindo a retoma de funções importantes (mas não essenciais) que possam ter sido temporariamente suspensas.

47. O plano de continuidade operacional deverá definir as condições para iniciar a recuperação, identificar a autoridade habilitada a autorizar a transição e especificar as medidas necessárias para regressar em segurança às operações normais.

48. Na fase de recuperação, há que considerar os seguintes pontos:

(a) *Verificação das condições para a recuperação*. Antes de efetuar a transição, o PCN deverá avaliar se o evento de perturbação subjacente foi resolvido ou suficientemente atenuado; se as instalações principais, os sistemas de TIC e os canais de comunicação estão novamente plenamente operacionais; e se a integridade das bases de dados e dos documentos foi verificada. Deverá ser dada especial atenção aos dados reproduzidos durante a perturbação, a fim de evitar a perda de informações geradas durante a vigência dos mecanismos de continuidade operacional;

(b) *Transição faseada das funções essenciais*. As funções essenciais não deverão ser transferidas de volta de uma só vez. O PCN deverá ponderar a sua transferência por ordem inversa de prioridade, começando pelas funções em que uma breve interrupção durante a transição é mais tolerável, mantendo simultaneamente as funções de máxima prioridade ao abrigo dos mecanismos de continuidade até que se confirme a estabilidade do ambiente normal. Durante a transição, é importante recorrer ao funcionamento em paralelo para reduzir o risco de falha em cascata;

(c) *Retoma de funções importantes*. As funções não essenciais que tenham sido temporariamente suspensas durante a perturbação só deverão ser retomadas quando for confirmado que as funções essenciais estão estáveis ao abrigo dos procedimentos normais. A ordem e o ritmo de retoma deverão ser ajustados à disponibilidade do pessoal, tendo em conta que os mecanismos de continuidade operacional aumentam frequentemente a carga de trabalho e a fadiga do pessoal;

(d) *Verificação de vulnerabilidades adicionais*. O PCN deverá verificar se os mecanismos de continuidade operacional não introduziram vulnerabilidades adicionais antes de regressar ao funcionamento normal.

49. O PCN deverá também realizar as seguintes atividades:

(a) *Reunião de balanço após o evento*. Para ajudar a identificar o que funcionou e o que não funcionou, o PCN deverá agendar uma reunião de balanço que envolva todas as categorias de pessoal que participaram na resposta;

(b) *Documentação pós-ação*. O PCN deverá elaborar um documento pós-ação estruturado que resuma a sequência dos eventos, a ativação dos mecanismos de continuidade operacional, o desempenho das funções essenciais, as lacunas observadas e os ensinamentos identificados;

(c) *Integração dos ensinamentos identificados no plano de continuidade operacional*. Após cada evento de perturbação que desencadeie a ativação do plano de continuidade operacional, o PCN deverá estabelecer um prazo definido para a atualização do plano, de modo que os ensinamentos identificados sejam incorporados antes de se perderem da memória operacional. Por conseguinte, o PCN deverá estabelecer um processo para acompanhar as deficiências identificadas e as medidas corretivas, bem como para voltar a testar as medidas atualizadas, conforme adequado. Se for caso disso, os ensinamentos identificados deverão também traduzir-se em melhorias nas atividades habituais do PCN.

3.14. **Estratégia de comunicação**

50. A gestão eficiente de eventos de perturbação passa pela comunicação, e cada PCN deverá desenvolver uma estratégia de comunicação sólida que reconheça as suas responsabilidades tanto na comunicação geral como na comunicação em situações de crise. Esta estratégia deverá orientar as decisões e ações do PCN em matéria de partilha de informações durante as perturbações, assegurando que todas as partes envolvidas ou afetadas recebem as informações necessárias e, se for caso disso, são capazes de agir em conformidade, ajudando assim a proteger a reputação da organização e a manter a confiança. O anexo VI apresenta sugestões de pontos a ter em conta pelo PCN ao elaborar uma estratégia de comunicação sólida.

4. **RECOMENDAÇÕES PARA A ORGANIZAÇÃO E REALIZAÇÃO DE UM TESTE DE ESFORÇO**

51. A Comissão recomenda a realização de testes de esforço aos PCN no âmbito do MPCU. A presente secção fornece orientações sobre a forma de conceber e avaliar um teste de esforço.

4.1. **Finalidade e objetivos**

52. O objetivo do teste de esforço deverá ser avaliar a capacidade do PCN para continuar a desempenhar as suas funções essenciais em condições de perturbação. Para o efeito, o teste de esforço deverá assumir a forma de um exercício em escala limitada destinado a avaliar os mecanismos de continuidade operacional existentes e o desempenho de funções essenciais específicas do PCN em condições de perturbação, nomeadamente através do teste de recursos tanto primários como alternativos.

53. O teste de esforço deverá visar os seguintes objetivos gerais:

(a) Rever, atualizar e validar o plano de continuidade operacional, bem como avaliar os conhecimentos especializados, os equipamentos e as disposições do PCN relacionados com a continuidade operacional;

(b) Melhorar a compreensão das prioridades e dos condicionalismos, bem como alterar as perceções relativamente à continuidade operacional do PCN;

(c) Identificar deficiências, lacunas, estrangulamentos e dependências, bem como oportunidades de melhoria do plano de continuidade operacional e nos recursos que sustentam as funções essenciais, na formação conexa, nos equipamentos e nas disposições do PCN;

(d) Avaliar a capacidade do pessoal essencial do PCN a vários níveis, incluindo a direção, para desempenhar as suas funções e responsabilidades;

(e) Avaliar a coordenação e a comunicação dentro da organização e com parceiros externos em condições de perturbação.

54. Ao planear o teste de esforço, recomenda-se a formulação de objetivos específicos que sejam mensuráveis e alinhados com as funções essenciais a testar.

55. O teste de esforço não deverá ter por objetivo identificar ameaças suscetíveis de desencadear incidentes que possam perturbar o funcionamento normal do PCN.

4.2. **Âmbito**

56. O âmbito do teste de esforço deverá identificar o seguinte:

(a) Os objetivos específicos do teste de esforço;

(b) As funções essenciais a avaliar;

(c) A natureza e a duração da perturbação que afeta a continuidade das operações;

(d) Os recursos envolvidos, incluindo os membros do pessoal e as suas funções, as instalações, os equipamentos e os sistemas de TIC;

(e) O grau de envolvimento das partes interessadas externas.

4.3. **Cenário**

57. Uma abordagem baseada em cenários deverá abranger as consequências de incidentes (fatores de desencadeamento) que possam causar perturbações nas operações e, por conseguinte, fazer ativar o plano de continuidade operacional do PCN. Recomenda-se que sejam testados diferentes cenários e níveis de complexidade, preparando assim a organização para uma série de resultados possíveis. Importa assegurar que os cenários sejam desafiantes, mas realistas, de modo a proporcionar informações significativas sobre a eficácia do plano de continuidade operacional. O anexo VII apresenta dois exemplos de cenários.

58. Recomenda-se que os PCN que utilizem a seguinte lista não exaustiva de fatores de desencadeamento para a ativação do plano de continuidade operacional do PCN: indisponibilidade de instalações (1), perturbação do fornecimento de eletricidade (2), perturbação ou falha dos sistemas de TIC (3) e faltas de pessoal em grande escala e faltas de pessoal essencial escasso (4).

(a) *Fator de desencadeamento 1: indisponibilidade das instalações*. O edifício onde se situava o PCN sofreu danos físicos, está inacessível ou foi evacuado. Estas circunstâncias tornam-no inutilizável por um período de tempo indeterminado.

(b) *Fator de desencadeamento 2: rutura do fornecimento de eletricidade*. Uma falha na rede elétrica deixa o edifício onde o PCN opera sem eletricidade. Esta interrupção do fornecimento de energia persiste para além do tempo de funcionamento do gerador de reserva do PCN antes de este necessitar de reabastecimento de combustível. Se a duração exata da autonomia de combustível do gerador for desconhecida, a interrupção deverá ser tratada como sendo por tempo indeterminado.

(c) *Fator de desencadeamento 3: perturbação ou falha dos sistemas de TIC*. Em resultado de uma falha no sistema de TIC, o *software* ou a(s) aplicação(ões) do PCN não conseguem funcionar eficazmente. Esta falha também impede o acesso a bases de dados essenciais, deixando os sistemas de TIC inoperacionais por um período indeterminado.

(d) *Fator de desencadeamento 4: faltas de pessoal em grande escala ou faltas de pessoal essencial escasso*. Uma parte significativa do pessoal fica subitamente impossibilitada de desempenhar as suas funções. Esta escassez pode incluir a ausência de pessoal essencial escasso e resultar em atrasos ou perturbações nas operações. Prevê-se que a duração desta indisponibilidade seja suficientemente longa para ultrapassar a capacidade de sobrecarga de trabalho do pessoal restante.

59. Os testes de esforço deverão combinar progressivamente vários eventos de perturbação para avaliar a capacidade de o PCN manter as funções essenciais durante perturbações em cascata ou combinadas que afetem vários recursos em simultâneo.

4.4. **Participantes**

60. Recomenda-se a identificação dos participantes de acordo com os objetivos definidos, as funções essenciais e o cenário do teste de esforço.

4.5. **Avaliação, identificação dos ensinamentos e aplicação de melhorias**

61. Ao planear o teste de esforço, é aconselhável estabelecer um sistema de avaliação. Tal ajuda a identificar lacunas e áreas de melhoria no plano de continuidade operacional, ao mesmo tempo que permite avaliar o sucesso global do exercício. Proporciona igualmente uma base para o planeamento e a formação futura em matéria de continuidade operacional do PCN.

62. Recomenda-se que o formato de avaliação seja sistematizado, tanto após eventos reais como após exercícios ou atividades de formação, incluindo testes de esforço. Para efeitos do teste de esforço, recomenda-se que os PCN utilizem a grelha de avaliação constante do anexo VIII. A referida grelha de avaliação sugere que a continuidade operacional seja avaliada sob duas perspetivas complementares:

(a) *A conformidade com o plano de continuidade operacional*; e

(b) *A manutenção das funções essenciais, bem como o cumprimento dos objetivos de desempenho predefinidos.*

63. Além disso, o quadro constante do anexo IX destina-se a apoiar os PCN na elaboração da avaliação, na identificação de ensinamentos e nas propostas de melhorias. O anexo X contém um modelo de questionário destinado a recolher os comentários dos participantes.

64. Os Estados-Membros e os Estados participantes no MPCU são convidados a partilhar com o CCRE os ensinamentos não sensíveis retirados e as melhorias propostas após a realização de um teste de esforço ao seu PCN.

Feito em Bruxelas, em 29 de outubro de 2026.

Pela Comissão
Hadja LAHBIB
Membro da Comissão

ANEXO I

Categorias de eventos de perturbação

Podem ser identificadas quatro categorias diferentes de eventos de perturbação para efeitos de continuidade operacional e de testes de esforço dos PCN no âmbito do MPCU:

— *Indisponibilidade das instalações:* as instalações do PCN já não podem ser utilizadas devido a um incidente físico ou operacional que impede ou limita gravemente o acesso ao edifício ou a sua utilização, seja de forma temporária ou permanente. Os exemplos incluem também o bloqueio das principais vias de acesso, danos físicos em edifícios próximos e falhas ou problemas que afetem os serviços públicos essenciais e as instalações, como os sistemas de fornecimento de água, de aquecimento, de ventilação ou de segurança ([1]). Os referidos incidentes também podem perturbar a atividade normal do PCN, obrigando à evacuação das instalações, impedindo o acesso às mesmas ou a sua utilização.

— *Rutura do fornecimento de eletricidade*: uma falha de energia que afeta as instalações do PCN. Uma falha prolongada no fornecimento de energia pode provocar um incidente a nível do abastecimento de combustível para os geradores de reserva. Pode também ter impacto nos sistemas dependentes da eletricidade, incluindo os sistemas de TIC.

— *Perturbação ou falha dos sistemas de TIC:* o *software* ou as aplicações do PCN não conseguem funcionar eficazmente. Uma falha deste tipo pode assumir várias formas, como a perda de acesso devido a problemas de autenticação, uma degradação grave do desempenho, a corrupção ou indisponibilidade de dados, a falha das interfaces com sistemas externos ou a perturbação na sequência de atualizações ou de um incidente de cibersegurança, incluindo casos como a personificação ilícita de um sistema principal do PCN, conduzindo à disseminação pelo PCN de informações manipuladas.

— *Faltas de pessoal em grande escala ou faltas de pessoal essencial escasso*: um número significativo de membros do pessoal essencial não consegue chegar às instalações ou está impossibilitado de trabalhar por qualquer motivo. A situação é agravada quando as funções essenciais dependem de um único indivíduo ou de um pequeno grupo de pessoal essencial escasso, cuja ausência ou indisponibilidade imprevista causa perturbações.

Estas quatro categorias proporcionam um quadro para compreender as medidas necessárias para atenuar as perturbações. No entanto, os eventos de perturbação podem também ser desencadeados por outros incidentes, como um afluxo súbito de informações que exceda a capacidade do PCN para as gerir, ou a divulgação de informações falsas que exija a mobilização de recursos do PCN para verificar e divulgar informações corretas.

Além disso, os eventos de perturbação podem estar interligados, e um único evento de perturbação pode afetar várias zonas em simultâneo. Por exemplo, um incêndio pode tornar as instalações inacessíveis, causando simultaneamente um corte de energia e danificando os sistemas de TIC e os dados. Podem também resultar de ações intencionais ou maliciosas, incluindo ciberincidentes e atividades híbridas, e de vários incidentes concomitantes, o que intensifica o seu impacto global. Consequentemente, os PCN têm de desenvolver um plano de resposta abrangente que aborde cada categoria individualmente, tenha em conta os seus efeitos combinados e se prepare para a possibilidade de perturbações simultâneas, a fim de assegurar a continuidade das suas operações.

([1]) A rutura do fornecimento de eletricidade e a perturbação ou falha dos sistemas de TIC são consideradas categorias diferentes.

ANEXO II

Exemplos de objetivos de desempenho operacional

Capacidade	Objetivo operacional indicativo (a avaliar e adaptar aos requisitos nacionais)
Conhecimento da situação inicial	no prazo de 15 minutos
Ativação dos mecanismos de continuidade	no prazo de 30 minutos
Estabelecimento de comunicações alternativas	no prazo de 30 minutos
Local alternativo para o comando operacional	no prazo de 2 horas
Capacidade de apoio à decisão	ininterruptamente, sempre que possível
Autonomia de combustível	no mínimo, de 72 horas
Autonomia em alimentos e água	no mínimo, de 72 horas
CECIS operacional	no prazo de 60 minutos
Primeiro relatório de situação operacional ao CCRE	no âmbito do primeiro ciclo de apresentação de relatórios operacionais

ANEXO III

Quadro de apoio à análise dos processos operacionais

Função essencial 1	*Designação da função.*
Descrição	*Incluir uma descrição desta função, incluindo as tarefas que a compõem.*
Recursos	*Enumerar os recursos (informações, conjuntos de dados, serviços, produtos, fornecimentos, disposições orçamentais, equipamentos, sistemas de TIC e requisitos de localização) necessários para desempenhar esta função e, se for caso disso, as entidades externas que os fornecem.*
Resultados	*Enumerar as informações, produto(s), serviço(s) ou ação(ões) resultantes desta função e identificar a(s) organização(ões) [externa(s)], entidade(s) grupo(s) que os recebe(m).*
Liderança (validação ou autorização)	*Enumerar os cargos com funções de validação ou autorização necessárias para executar esta função, se aplicável.*
Pessoal essencial	*Enumerar os cargos do pessoal essencial, bem como o seu perfil, conhecimentos especializados e formação, se for caso disso, nomeadamente a credenciação de segurança.*
Instalações	*Enumerar o(s) local(is) físico(s) ou as instalações onde a função essencial é desempenhada.*
Equipamentos e sistemas	*Enumerar os equipamentos, sistemas e meios necessários para realizar esta função. Estes podem incluir instalações seguras, computadores para comunicações encriptadas, paredes de vídeo, salas de reunião de alto nível, equipamentos de videoconferência e computadores com acesso aos Serviços Transeuropeus de Telemática entre as Administrações (TESTA), etc.*
Registos essenciais	*Enumerar os dados e as informações necessárias para desempenhar a função.*
Dependências e interdependências	*Enumerar as relações ou os acordos entre os elementos acima identificados e especificar, se for caso disso, a natureza da relação ou do acordo, os serviços essenciais necessários (por exemplo, fornecimento de energia, TIC, etc.), o impacto em caso de perturbação do serviço ou do fornecimento e os acordos com as entidades que prestam esses serviços ou fornecimentos. A avaliação deverá também descrever as interdependências, incluindo os efeitos em cascata, sempre que a perturbação de um serviço (por exemplo, eletricidade ou TIC) afete outros serviços, amplificando assim o impacto operacional.*
Reservas	*Enumerar os recursos ou mecanismos alternativos que seriam ativados para manter o funcionamento se os principais recursos ou mecanismos fossem afetados pelo evento de perturbação.*

ANEXO IV

Orientações para a aplicação de medidas de atenuação e prevenção

A presente secção fornece orientações para a aplicação de medidas de atenuação e prevenção, organizadas por categoria de eventos de perturbação. Para evitar repetições, as medidas aplicáveis a várias categorias diferentes de eventos de perturbação são descritas apenas uma vez na primeira categoria aplicável.

— Indisponibilidade das instalações:

— *Distribuição geográfica do PCN por dois ou mais centros geograficamente separados que funcionem em simultâneo, assegurando o apoio mútuo e salvaguarda em caso de carga excessiva de trabalho*. Cada local deverá funcionar 24 horas por dia e estar totalmente equipado para gerir toda a carga de trabalho caso o ou os outros locais fiquem temporariamente inoperacionais. Além disso, os locais devem ser escolhidos com base numa análise de risco e de acessibilidade das diferentes zonas, devendo os locais principais e alternativos situar-se em zonas de risco distintas e dispor de diferentes vias de acesso. Por exemplo, em zonas propensas a sismos, os locais deverão situar-se em diferentes placas tectónicas; em zonas propensas a inundações, deverão situar-se a altitudes significativamente diferentes ou em bacias hidrográficas diferentes.

— *Relocalização para instalações alternativas geridas pela autoridade do PCN*. Ponderar a possibilidade de estabelecer, pelo menos, dois locais alternativos. Um deles deverá ficar perto das instalações principais, a fim de facilitar a rápida relocalização e o pronto restabelecimento das funções essenciais. O outro deverá estar suficientemente distante para garantir que eventos de perturbação com grande impacto, como inundações ou tempestades de neve, não afetem ambos os locais simultaneamente. Garantir a segurança da informação e das comunicações, bem como a compatibilidade dos equipamentos e sistemas de TIC críticos — como o CECIS ou os equipamentos necessários para as comunicações classificadas — tanto nas instalações principais como nas instalações alternativas.

— *Transporte previamente organizado para o pessoal essencial até às instalações alternativas (nomeadamente em condições meteorológicas adversas)*. A fim de assegurar um nível de pessoal adequado, estabelecer disposições para o transporte de pessoal essencial em caso de ativação do plano de continuidade operacional com a utilização de instalações alternativas ou unidades móveis remotas. Ter em conta o potencial impacto nas vias de transporte, como o congestionamento do trânsito e o bloqueio devido a condições meteorológicas adversas, falhas nas infraestruturas, perturbação da ordem pública ou outras causas.

— *Trabalho à distância (que implica flexibilidade nas tarefas que podem ser realizadas fora do local físico do PCN)*. Identificar as funções ou etapas essenciais que fazem parte das funções essenciais que podem ser desempenhadas à distância. Tal poderá ser possível porque essas funções/etapas não dependem de equipamentos ou sistemas exclusivos das instalações físicas principais. Ponderar a criação de um plano ou sistema de contingência para reestruturar as responsabilidades do pessoal, permitindo que alguns membros do pessoal trabalhem a partir de casa, enquanto outros são transferidos para as instalações alternativas.

— *Unidades móveis de comando e controlo que possam acolher temporariamente o pessoal essencial do PCN*. Estas unidades deverão permitir a execução de funções essenciais a partir de um ambiente móvel, incluindo o acesso aos sistemas de informações operacionais e ao CECIS. Importa definir os equipamentos e o nível de autossuficiência necessários para garantir a prontidão operacional. Estas unidades deverão ser concebidas para assegurar temporariamente as operações das instalações principais durante um período predefinido.

— *Ativação de acordos administrativos com outras autoridades para utilização das suas instalações*. Celebrar acordos com outras autoridades nacionais ou infranacionais para a utilização partilhada temporária das suas instalações. Avaliar a configuração, os sistemas, os equipamentos e as medidas de segurança necessárias para desempenhar eficazmente as funções essenciais. Assegurar que estes acordos incluam exercícios e testes regulares para validar a prontidão e a adequação destas instalações alternativas.

— *Descentralização de poderes*. Assegurar a existência de mecanismos e estabelecer um sistema para delegar funções noutras autoridades nacionais.

— Rutura do fornecimento de eletricidade:

— *Ativação de geradores e de unidades de alimentação ininterrupta (UPS)*. Fornecer geradores e sistemas UPS dimensionados para assegurar a continuidade das funções essenciais do PCN durante um período mínimo definido. A sua capacidade deverá ser suficiente para satisfazer as necessidades operacionais em caso de cortes de energia prolongados. Os geradores e os sistemas UPS deverão ser testados regularmente para garantir a sua prontidão operacional.

— *Acordos e contratos de fornecimento prioritário de combustível com fornecedores*. Os acordos relativos ao fornecimento de combustível deverão garantir a continuidade das operações e basear-se na capacidade de armazenamento de combustível no local, bem como no consumo de combustível previsto. As medidas adicionais podem incluir a disponibilidade de reservatórios móveis de combustível com sistemas de bombagem e/ou acordos de fornecimento prioritário com fornecedores de combustível próximos.

— *Autonomia energética e fontes de energia alternativas para funções essenciais*. Sempre que possível, o PCN deverá poder funcionar independentemente da rede elétrica nacional. Se a rede elétrica falhar durante vários dias, como pode acontecer em caso de grandes catástrofes, a continuidade poderá ser assegurada através de fontes de energia diversificadas e de uma microrrede autossuficiente, por exemplo, uma microrrede eólica ou solar. Ponderar a instalação de fontes de energia alternativas, como painéis fotovoltaicos com armazenamento em baterias, dimensionadas para alimentar as funções essenciais do PCN.

— *Maximização da capacidade de energia disponível*. Estabelecer protocolos internos para maximizar a capacidade de energia disponível, restringindo a utilização de equipamentos não essenciais e desligando progressivamente as cargas não necessárias para apoiar as funções essenciais, prolongando assim a autonomia de energia de reserva sem investimento adicional.

— *Relocalização para instalações alternativas geridas pela autoridade do PCN com fornecimento de eletricidade* (ver as recomendações relevantes da secção «Indisponibilidade das instalações»)

— *Trabalho à distância a partir de um edifício com fornecimento de eletricidade garantido* ver as recomendações relevantes da secção «Indisponibilidade das instalações»)

— *Unidades móveis de comando e controlo autossuficientes em termos de eletricidade* (ver as recomendações relevantes da secção «Indisponibilidade das instalações»)

— *Ativação de acordos administrativos com outras autoridades para utilização das suas instalações com fornecimento de eletricidade garantido* (ver as recomendações relevantes da secção «Indisponibilidade das instalações»)

— *Descentralização de poderes* (ver as recomendações relevantes da secção «Indisponibilidade das instalações»)

— Perturbação ou falha dos sistemas de TIC:

— *Redundância*. A redundância garante que a falha de um componente não interrompe a função que este assegura. O PCN deverá aplicar a redundância a níveis complementares: i) equipamentos (duplicar componentes essenciais), ii) conectividade (múltiplos fornecedores e diferentes vias de acesso e iii) aplicações e dados (replicação de bases de dados e documentos essenciais para um local secundário). Os mecanismos de redundância deverão ter capacidade suficiente para manter as operações em caso de falha do principal ambiente de TIC e deverão ser testados periodicamente para assegurar a prontidão e a comutação automática sem descontinuidades em caso de perturbação. Devem evitar dependências partilhadas com o sistema principal, como as mesmas fontes de alimentação, fornecedores ou infraestruturas físicas que possam falhar simultaneamente.

— As linhas de fibra ótica são altamente vulneráveis a movimentos do solo, o que pode causar atenuação ou perda do sinal e interrupções de serviço. Para atenuar este risco, recomenda-se a comutação automática por satélite como medida de redundância padrão, permitindo que a rede de reserva mantenha o mesmo conhecimento da situação que a rede primária. A espelhagem geográfica de dados deve ser do tipo ativo-ativo, mantendo os ambientes primário e de reserva sincronizados, para que ambos possam assumir o controlo sem descontinuidades. Esta abordagem de redundância e espelhagem contribuem para elevados níveis de disponibilidade e desempenho nas redes de fibra ótica.

— *Cópias de segurança de dados regulares e seguras, incluindo cópias fora do local e fora de linha*. Estabelecer e manter uma política de cópias de segurança estruturada para todos os dados e configurações essenciais para as operações do PCN. Esta política deverá definir o que é objeto de cópia de segurança, com que frequência, o local onde as cópias de segurança são armazenadas (incluindo cópias fora do local ou fora de linha) e quem é responsável pela sua gestão. As cópias de segurança deverão ser encriptadas e protegidas contra o acesso não autorizado.

— *Sistemas de TIC e canais de comunicação alternativos*. Criar ferramentas e canais alternativos que possam ser utilizados em caso de falha dos sistemas de TIC ou redes principais. Estes podem incluir comunicações por satélite, unidades de radiocomunicações móveis de alta frequência (HF), de muito alta frequência (VHF) ou de ultra-alta frequência (UHF), linhas telefónicas analógicas, aplicações de mensagens seguras ou plataformas baseadas na Web alojadas fora da infraestrutura principal. O pessoal deverá saber quando e como mudar para estas alternativas.

— *Equipas de apoio de TIC de emergência ou unidades técnicas de resposta permanente*. Providenciar um acesso rápido ao apoio no domínio das TIC, quer prestado internamente (dentro da organização) quer por um prestador externo, definindo mecanismos claros de disponibilidade e de resposta, de modo que a assistência técnica possa ser mobilizada rapidamente quando necessário para assegurar a rápida recuperação dos sistemas de TIC.

— *Procedimentos de resposta a ciberincidentes coordenados com a autoridade nacional de cibersegurança*. Estabelecer protocolos de coordenação com a autoridade nacional de cibersegurança, incluindo canais de alerta precoce, procedimentos conjuntos de resposta a incidentes e funções e responsabilidades claramente definidas durante um ciberincidente que afete o PCN.

— *Cópias fora de linha das listas de contactos essenciais, dos principais procedimentos e dos documentos operacionais;* Informações como listas de contactos, procedimentos relativos a incidentes e modelos principais deverão estar disponíveis em formatos que possam ser utilizados sem acesso aos principais sistemas de TIC.

— *Unidades móveis de comando e controlo com acesso aos sistemas de TIC principais e de reserva* (ver as recomendações relevantes da secção «Indisponibilidade das instalações»).

— *Relocalização para instalações alternativas geridas pela autoridade do PCN com acesso aos sistemas de TIC principais e de reserva* (ver as recomendações relevantes da secção «Indisponibilidade das instalações»).

— *Ativação de acordos administrativos com outras autoridades para utilização das suas instalações com acesso aos sistemas de TIC* (ver as recomendações relevantes da secção «Indisponibilidade das instalações»).

— Faltas de pessoal em grande escala ou faltas de pessoal essencial escasso:

— *Gestão das horas extraordinárias (solução a curto prazo)*. Estabelecer um protocolo de horas extraordinárias que defina: critérios claros relativamente à utilização de horas extraordinárias; quem as pode autorizar; limites definidos (duração máxima do turno, número máximo de horas semanais e número máximo de dias consecutivos); períodos mínimos de descanso entre turnos e após atingir o número máximo de horas semanais ou o número máximo de dias consecutivos; um sistema de rotação justo, de modo que o mesmo pessoal não seja repetidamente solicitado; um sistema de registo das horas extraordinárias; remuneração adicional preestabelecida; e apoio prático durante horários prolongados (por exemplo, refeições, áreas de descanso e transporte para casa, se necessário).

— *Reafetação de tarefas essenciais ao pessoal disponível*. Preparar mecanismos de contingência que especifiquem a forma como as funções essenciais serão redistribuídas na ausência de pessoal-chave. Tal inclui a identificação de pessoal substituto para cada função essencial e a simplificação dos procedimentos, sempre que possível.

— *Uma reserva pré-identificada de pessoal formado dentro da instituição, disponível num curto espaço de tempo*. Criar um sistema para mobilizar pessoal de apoio a partir de uma reserva pré-identificada, definindo regras claras sobre quem pode mobilizar esse pessoal e de que forma, incluindo critérios de ativação, canal(is) de comunicação para a mobilização, requisitos relativos ao pessoal (como credenciação de segurança, formação ou conhecimentos especializados) e a forma como as folgas ou as horas extraordinárias são geridas, com revisões periódicas para garantir o bom funcionamento do sistema. Assegurar que estas regras são bem conhecidas entre o pessoal da reserva.

— Esta reserva pode ser constituída através de: i) formação cruzada do pessoal de outras unidades — implementar programas de formação cruzada para que vários membros do pessoal possam desempenhar as mesmas funções essenciais, centrando-se em funções identificadas como estrangulamentos; e ii) uma «reserva latente» de antigos membros do pessoal essencial do PCN — rotação do pessoal para prestar serviço noutros departamentos após um determinado período, de forma criar uma reserva latente de pessoal. A manutenção desta reserva latente proporciona uma maior capacidade em termos de pessoal e permite uma mobilização rápida, evitando os meses de formação e de verificação de segurança normalmente necessários para funções tão sensíveis. Em ambos os casos, deverão ser formalizados procedimentos para assegurar que o pessoal da reserva se mantenha atualizado através de formação de atualização periódica e possa ser rapidamente mobilizado em caso de crise grave.

— *Priorização do recrutamento de pessoal*. O funcionamento contínuo dos PCN, 24 horas por dia, sete dias por semana, exige níveis estáveis de pessoal. O PCN pode ponderar a possibilidade de dar prioridade ao recrutamento para funções de apoio a funções essenciais e de antecipar a escassez previsível de pessoal (por exemplo, aposentações simultâneas ou contratos a termo certo que terminam), de modo a iniciar o recrutamento com antecedência suficiente. As medidas podem incluir o desenvolvimento de processos de recrutamento céleres. Além disso, a formação contínua do pessoal existente pode contribuir ainda mais para a estabilidade do pessoal, permitindo a mobilidade interna, o desenvolvimento de competências e a sucessão em funções essenciais.

— *Investimento na retenção de pessoal essencial*. Para reter o pessoal que trabalha nos PCN, a motivação deverá ser fomentada através de uma combinação de benefícios e incentivos. Os incentivos não monetários podem incluir licenças prolongadas após um determinado período de serviço, regimes de escalas de serviço flexíveis, sujeitos a requisitos mínimos de cobertura do serviço, zonas de descanso no local, medidas de apoio à família (por exemplo, acesso a acolhimento de crianças) e acesso a serviços com desconto ou gratuitos, como transportes públicos, cuidados de saúde e instalações culturais ou desportivas.

— *Apoio às famílias do pessoal essencial*. A disponibilidade do pessoal essencial pode depender das suas famílias, em especial se estas estiverem em risco ou sem assistência. Ponderar a adoção de disposições, se for caso disso, para proteger as famílias do pessoal essencial do PCN, dando prioridade à sua segurança, para que o pessoal possa permanecer operacional.

— *Prevenção de estrangulamentos devido a falta de pessoal através da delegação de poderes e da promoção de uma responsabilidade partilhada*. Assegurar que as responsabilidades e tarefas estão claramente definidas. Estabelecer protocolos para a delegação de poderes. Identificar os sucessores com os respetivos cargos, que interviriam caso os decisores responsáveis pelas funções essenciais não estivessem disponíveis. Especificar as circunstâncias e a ordem em que assumiriam essas funções. Sempre que a decisão e as responsabilidades o permitam, assegurar o reforço das capacidades e a formação regular para assumir a autoridade em caso de perturbação. Ponderar se a distribuição ou partilha de responsabilidades entre vários membros do pessoal através de um sistema de rotação é viável e útil para evitar estrangulamentos. Ponderar a manutenção de um manual atualizado para os novos membros do pessoal, concebido para permitir que os colegas menos experientes consigam gerir de forma autónoma uma vasta gama de tarefas, assegurando simultaneamente o cumprimento das normas e dos protocolos estabelecidos.

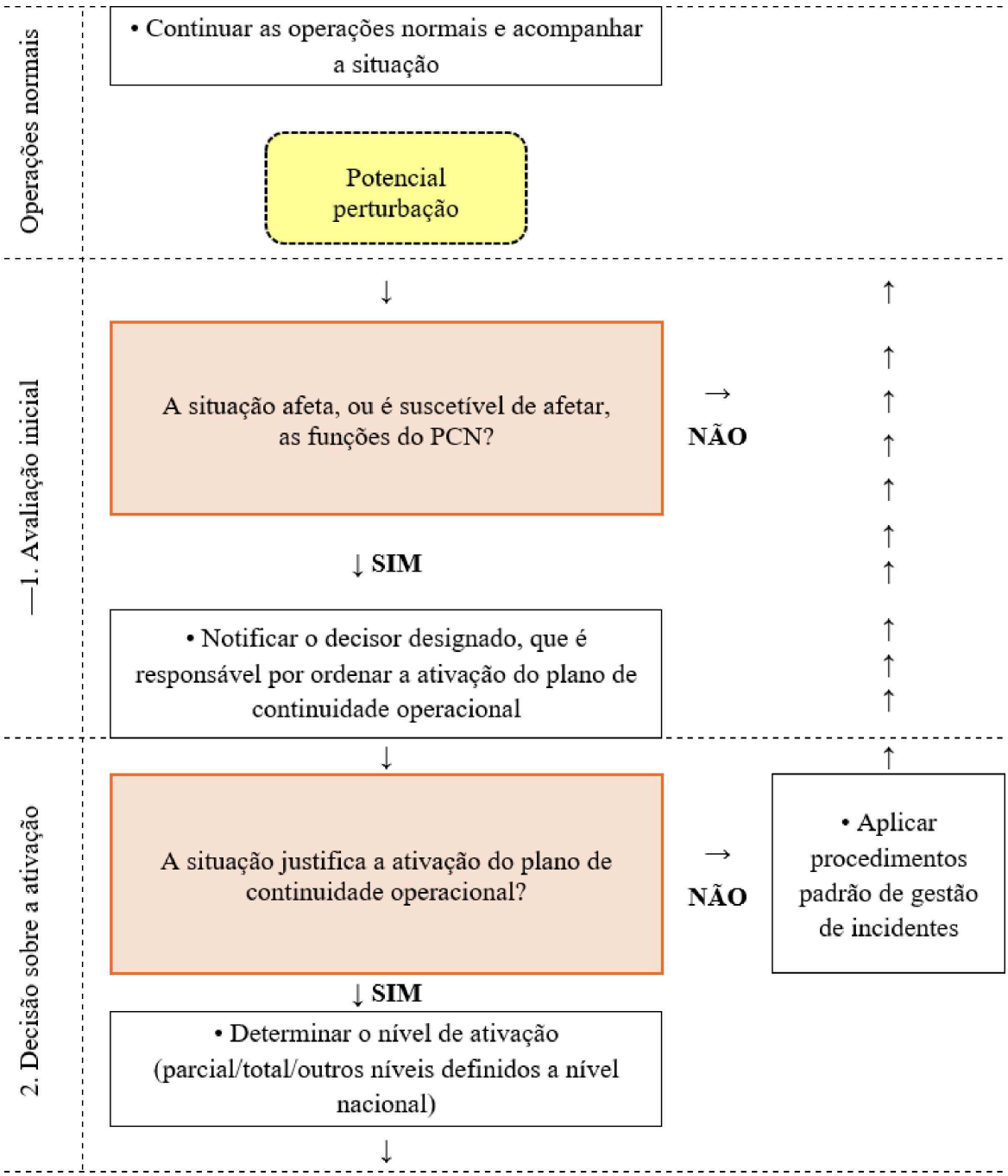
ANEXO V

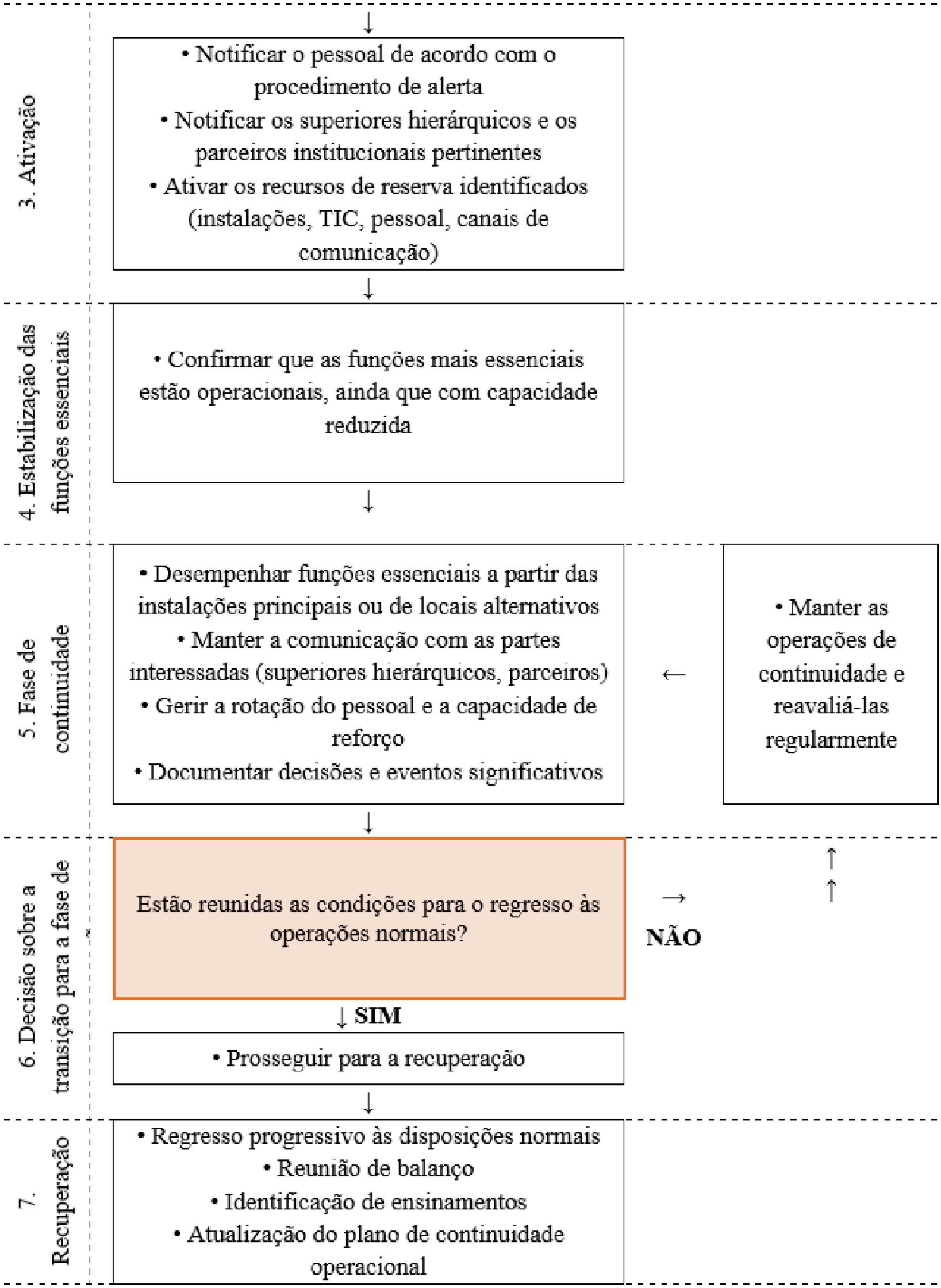
Ferramentas de referência operacionais

O presente anexo fornece uma ferramenta de referência operacional que os PCN deverão ponderar utilizar aquando da elaboração ou revisão do seu plano de continuidade operacional.

Exemplo de fluxo de ativação

O fluxo apresentado abaixo é um exemplo de como a ativação de um plano de continuidade operacional pode ser organizada, desde o momento em que é detetada uma potencial perturbação até o PCN entrar numa fase de continuidade estável. Está estruturado em torno de pontos de decisão e não de prazos predefinidos.




3. Ativação
• Notificar o pessoal de acordo com o procedimento de alerta
• Notificar os superiores hierárquicos e os parceiros institucionais pertinentes
• Ativar os recursos de reserva identificados (instalações, TIC, pessoal, canais de comunicação)
4. Estabilização das funções essenciais
• Confirmar que as funções mais essenciais estão operacionais, ainda que com capacidade reduzida
5. Fase de continuidade
• Desempenhar funções essenciais a partir das instalações principais ou de locais alternativos
• Manter a comunicação com as partes interessadas (superiores hierárquicos, parceiros)
• Gerir a rotação do pessoal e a capacidade de reforço
• Documentar decisões e eventos significativos
←
• Manter as operações de continuidade e reavaliá-las regularmente
6. Decisão sobre a transição para a fase de recuperação
Estão reunidas as condições para o regresso às operações normais?
→ NÃO
↓ SIM
• Prosseguir para a recuperação
7. Recuperação
• Regresso progressivo às disposições normais
• Reunião de balanço
• Identificação de ensinamentos
• Atualização do plano de continuidade operacional

ANEXO VI

Principais pontos a abordar na elaboração de uma estratégia de comunicação [1]

— Identificar os diferentes públicos-alvo, no âmbito da responsabilidade da organização em matéria de comunicação, que poderiam ser potencialmente afetados pela perturbação das operações do PCN ou que teriam de ser informados caso a organização sofresse um evento de perturbação, incluindo:

  (a) Os níveis superiores da organização, nomeadamente o nível de tomada de decisões;

  (b) O pessoal da organização;

  (c) As partes interessadas que contribuem para as funções essenciais da organização;

  (d) As partes interessadas que recebem os resultados das funções essenciais da organização;

  (e) Os meios de comunicação social;

  (f) O público em geral.

— Para cada público-alvo, definir o objetivo da comunicação em caso de evento de perturbação. Cada público-alvo poderá necessitar de um tipo, formato e conteúdo de informação diferente. O(s) canal(is) de comunicação utilizado(s) também pode(m) ser diferente(s).

— Redigir mensagens predefinidas que sejam claras, concisas e coerentes para todos os destinatários, em todos canais e ao longo do tempo. Assegurar que são adaptadas ao público-alvo a que se destinam, dando resposta às suas necessidades específicas de informação.

— Identificar canais de comunicação alternativos para cada público-alvo, a fim de assegurar uma comunicação eficaz caso a perturbação afete os canais habituais.

— Considerar a informação proativa como uma melhor abordagem do que a informação reativa.

— Sempre que a estratégia de comunicação inclua a possibilidade de divulgar mensagens através da televisão e rádio pública, coordenar o momento de transmissão dessas mensagens com os noticiários, a fim de assegurar uma integração eficaz e uma ampla difusão junto da população.

— No âmbito da estratégia de comunicação, ponderar a atribuição prévia da função de gestor de informação a um determinado cargo, especificando as suas tarefas antes, durante e após um evento de perturbação.

[1] Estes pontos sugeridos para a elaboração de uma estratégia de comunicação não têm em conta a gestão das informações falsas ou da desinformação.

ANEXO VII

Exemplos de cenários

Exemplo de cenário 1

Evento: *falha de energia seguida de perda de dados.*

Onde: *a falha de energia afeta a zona onde se situam as instalações principais do PCN.*

Duração: *24 horas.*

Descrição: *as obras de reparação nas imediações das instalações do PCN causaram danos na rede de distribuição de eletricidade. O corte de energia repentino causou danos nos sistemas informáticos do PCN, resultando na perda de dados. Prevê-se que as obras de restabelecimento da energia durem 24 horas. A falha das TIC prolonga-se por 24 horas.*

Exemplo de cenário 2

Evento: *inacessibilidade das instalações devido a neve persistente.*

Onde: *toda a área onde se situam as instalações é afetada.*

Duração: *mais de uma semana.*

Descrição: *uma forte tempestade de neve atingiu a zona onde se situam as instalações do PCN, tornando-as inacessíveis por estrada e por transportes públicos. A queda de neve é tão intensa que os limpa-neves não conseguem desobstruir todas as estradas principais nas primeiras 24 horas, sendo dada prioridade ao acesso aos hospitais. Foi pedido à população que se mantivesse em casa. Durante pelo menos 48 horas, não será possível aceder às instalações do PCN por transportes públicos ou veículos particulares. A vaga de frio mantém-se na região há mais de uma semana e a neve nas estradas secundárias persiste há uma semana. Consequentemente, um terço do pessoal que deveria trabalhar nos dias seguintes não pode fazê-lo durante uma semana, uma vez que reside em locais remotos e as estradas secundárias são as últimas a serem desobstruídas.*

Além disso, o pessoal essencial que estava de serviço no dia da queda de neve ficou retido nas instalações durante as primeiras 48 horas. Cerca de um terço já atingiu o número máximo de horas que está autorizado a trabalhar nessa semana e outro terço atingirá esse limite nas próximas 24 horas. Por conseguinte, têm legalmente direito a um descanso adequado. Necessitam igualmente de apoio para satisfazer as necessidades básicas (alimentação, higiene pessoal) e, em alguns casos, de medidas de apoio às suas famílias e/ou de evacuação.

ANEXO VIII

Quadro de avaliação proposto para o teste de esforço

O resultado do teste de esforço deverá ser avaliado em função de duas dimensões distintas, mas complementares:

— *Conformidade com o plano de continuidade operacional*. Esta dimensão deverá avaliar em que medida o PCN aplicou os mecanismos de continuidade operacional durante o teste de esforço, incluindo as estruturas de tomada de decisão para a ativação, o escalonamento e a recuperação, a coordenação e comunicação interna e externa, as disposições sobre a relocalização e a utilização de recursos de reserva.

— *Manutenção das funções essenciais e cumprimento dos objetivos de desempenho operacional mensuráveis predefinidos*. Esta dimensão deverá avaliar se as funções essenciais do PCN foram mantidas ou retomadas dentro de limites predefinidos aceitáveis, se houve efeitos negativos noutras funções não essenciais do PCN e se o teste de esforço atingiu os objetivos de desempenho mensuráveis predefinidos. O anexo II apresenta exemplos de objetivos de desempenho operacional.

As duas dimensões deverão ser avaliadas separadamente, a fim de identificar com maior precisão as melhorias necessárias. Esta distinção ajuda a garantir que a conformidade com o plano de continuidade operacional é avaliada separadamente da eficácia do resultado operacional. O relatório de avaliação deverá apresentar o resultado sob a forma de duas pontuações complementares: uma que reflita a conformidade com o plano de continuidade operacional e outra que reflita a manutenção das funções essenciais e o cumprimento dos objetivos de desempenho operacional mensuráveis predefinidos.

Grelha de avaliação para avaliar a conformidade com o plano de continuidade operacional.

Classificação (0-3)	Descrição
0: não conformidade.	*O exercício revelou pouco ou nenhum alinhamento com os mecanismos de continuidade operacional. Os principais procedimentos estavam ausentes, foram executados incorretamente ou foram ignorados.*
1: conformidade parcial.	*Alguns pontos dos mecanismos de continuidade foram aplicados, mas outros pontos importantes não foram corretamente seguidos, foram aplicados demasiado tarde ou revelaram-se inadequados na prática. O teste revelou deficiências substanciais e importantes oportunidades de melhoria do plano.*
2: conformidade geral, apenas com pequenos desvios.	*De um modo geral, o teste de esforço foi executado em conformidade com o plano de continuidade operacional. Os desvios em relação ao plano foram limitados. O teste revelou algumas deficiências e oportunidades de melhoria do plano.*
3: plena conformidade.	*O plano de continuidade operacional foi integralmente seguido durante o teste de esforço.*

Grelha de avaliação para avaliar a manutenção das funções essenciais e o cumprimento dos objetivos de desempenho operacional mensuráveis predefinidos.

Classificação (0-3)	Descrição
0: não alcançados.	*As funções essenciais do PCN foram suspensas ou adiadas para além dos limites predefinidos aceitáveis. Outras funções não essenciais do PCN foram afetadas de forma significativa e negativa. Os objetivos de desempenho mensuráveis predefinidos não foram alcançados.*
1: alcançados, apesar de grandes dificuldades.	*Uma ou mais funções essenciais só foram restabelecidas após um atraso considerável, que excedeu os limites aceitáveis. O teste de esforço também poderá ter causado perturbações significativas ou afetado negativamente outras funções do PCN. Os objetivos de desempenho mensuráveis predefinidos foram alcançados apenas parcialmente ou com grandes dificuldades.*

Classificação (0-3)	Descrição
2: alcançados com pequenos desvios.	*As funções essenciais foram mantidas ou restabelecidas dentro de margens de tolerância aceitáveis (tendo os limites aceitáveis predefinidos sido excedidos por um período limitado), sem impacto significativo noutras funções do PCN. Os objetivos de desempenho mensuráveis predefinidos foram, em grande medida, alcançados, e apenas foram observados pequenos desvios em relação aos limites estabelecidos.*
3: plenamente alcançados.	*As funções essenciais abrangidas pelo teste de esforço foram mantidas ou restabelecidas sem atrasos que excedessem os limites aceitáveis predefinidos e sem impacto negativo noutras funções do PCN. Os objetivos de desempenho mensuráveis predefinidos foram plenamente alcançados.*

ANEXO IX

Avaliação do teste de esforço, identificação dos ensinamentos e melhorias propostas [1]

No processo de avaliação, é aconselhável identificar estratégias para melhorar os domínios em que não houve resposta adequada durante o exercício do teste de esforço. Além disso, os PCN deverão ponderar a incorporação de elementos bem-sucedidos que surgiram durante o exercício, mas que não estão incluídos no atual plano de continuidade operacional.

O quadro seguinte destina-se a facilitar a compilação e o alinhamento da avaliação, bem como a identificação dos ensinamentos e das melhorias propostas após a realização de um teste de esforço.

Conformidade com o plano de continuidade operacional.	*Classificação (0-3)*: … *Descrição*…
Manutenção das funções essenciais e cumprimento dos objetivos de desempenho operacional mensuráveis predefinidos.	*Classificação (0-3)*: … *Descrição*…
Conclusões e observações	…
Lacunas e ensinamentos identificados	…
Melhorias propostas	…
Ações necessárias para a aplicação	…

[1] O presente quadro de avaliação baseia-se no conjunto de instrumentos para recursos de continuidade desenvolvido pela Agência Federal de Gestão das Emergências (FEMA) dos EUA para apoiar as comunidades e as autoridades/organizações locais na elaboração de programas de continuidade operacional e foi adaptado ao exercício de teste de esforço.

ANEXO X

Formulário de comentários do participante

Recomenda-se o seguinte questionário como modelo para a recolha de comentários dos participantes nos testes de esforço. As perguntas deverão ser adaptadas ao âmbito e à incidência específica do teste de esforço. A recolha de respostas a estas ou a perguntas semelhantes junto dos participantes nos testes de esforço, dos observadores ou do pessoal envolvido em eventos de perturbação reais pode ajudar a identificar ensinamentos e lacunas, que podem depois ser utilizados para atualizar o plano de continuidade operacional do PCN.

Ativação do plano de continuidade operacional:

— Foram seguidos os protocolos estabelecidos?

— Em caso negativo, quais foram os motivos do desvio e este deveu-se a um erro/problema ou a um ajustamento positivo/de otimização?

— Quão eficiente foi a execução dos protocolos?

— Quais foram os desafios encontrados?

— A comunicação foi clara e eficaz durante a ativação?

— Todo o pessoal essencial foi notificado e mobilizado em tempo útil?

Retoma operacional, continuidade e desempenho das funções essenciais:

— Quanto tempo demorou a retomar as funções essenciais pelas quais é responsável?

— Todas as funções essenciais foram desempenhadas de forma eficiente e dentro dos prazos previstos? Avalie a qualidade dos resultados obtidos em condições de teste.

— Verificaram-se atrasos ou ineficiências no desempenho destas funções?

— Foi necessário dar prioridade a alguma função essencial durante o exercício?

— Como foi decidida e comunicada a definição de prioridades?

— A definição de prioridades foi eficaz para garantir a continuidade e a eficácia?

Equipamentos e sistemas de TIC:

— Todos os equipamentos de reserva necessários estavam disponíveis e plenamente operacionais?

— Os sistemas de reserva de fornecimento de eletricidade foram testados e estavam plenamente funcionais?

— As ferramentas e os canais de comunicação de reserva foram testados e estavam plenamente funcionais?

— Estavam disponíveis, foram testados e estavam plenamente operacionais outros serviços e recursos essenciais?

— Foram identificados atrasos ou ineficiências causadas pelos sistemas de TIC?

— Quão eficazmente foram resolvidos os problemas?

Instalações alternativas:

— O local alternativo é adequado em termos de dimensão, disposição e equipamento para lhe permitir trabalhar durante um longo período (vários dias)? Em caso negativo, porquê e o que poderia ser feito para melhorar a situação?

Comunicação e coordenação:

— Todos os participantes, incluindo os superiores hierárquicos e as equipas ou colegas pertinentes, foram devidamente informados?

— A comunicação e a coordenação interna foram mantidas de forma eficaz ao longo de todo o exercício, incluindo com os superiores hierárquicos?

— A comunicação e a coordenação com o CCRE foram mantidas de forma eficaz ao longo de todo o exercício?

— Se aplicável, quão eficaz foi a comunicação com o CCRE a partir do local alternativo?

— Como foram trocadas e documentadas as informações durante a relocalização ou a perturbação?

Formação e bem-estar do pessoal:

— Considera que estava bem preparado(a) para o exercício com base na formação de continuidade operacional realizada antes do mesmo?

— Recebeu informações suficientes sobre o exercício assim que este começou?

— Houve clareza quanto às funções durante o exercício?

— O exercício foi útil para fins de formação do pessoal?

— As suas necessidades pessoais e familiares foram tidas em conta, por exemplo, as suas necessidades de transporte, descanso, água ou alimentos?

Outras observações gerais:

— Que aspetos do exercício foram mais bem-sucedidos?

— Quais foram os principais desafios encontrados?

— O exercício cumpriu os seus objetivos?

— Com base na experiência adquirida durante o exercício, como avalia a capacidade do PCN para continuar a funcionar nas condições deste exercício durante uma semana?

— Identifique eventuais recursos ou apoios adicionais necessários para um evento de perturbação semelhante que dure mais tempo do que o exercício.

— Identifique melhorias para futuras ações de formação e exercícios.