BOLETIM OFICIAL

SET. 2021

Suplemento

BANCO DE PORTUGAL
EUROSISTEMA

BOLETIM OFICIAL DO BANCO DE PORTUGAL

9|2021 SUPLEMENTO

BANCO DE PORTUGAL
EUROSISTEMA

7 outubro 2021 • www.bportugal.pt • Legislação e Normas • SIBAP

BOLETIM OFICIAL DO BANCO DE PORTUGAL | Normas e informações 9|2021 SUPLEMENTO • Banco de Portugal
Av. Almirante Reis, 71 – 2.º | 1150-012 Lisboa • www.bportugal.pt • Edição Departamento de Serviços de Apoio |
Unidade de Documentação e Biblioteca • ISSN 2182-1720 (*online*)

Índice

Apresentação

O *Boletim Oficial* do Banco de Portugal, previsto no n.º 3 do artigo 59.º da sua Lei Orgânica, em formato eletrónico a partir de janeiro de 2012, tem como objetivo divulgar os diplomas normativos designados por Instruções, produzidos no exercício da sua competência regulamentar.

Acessoriamente, esta publicação reúne e disponibiliza os Avisos do Banco de Portugal (sempre publicados no *Diário da República*), as Cartas Circulares tidas como relevantes, bem como outras informações.

A sua periodicidade é mensal, sendo disponibilizado ao dia 15 de cada mês ou no primeiro dia útil seguinte, em www.bportugal.pt. Excecionalmente serão publicados suplementos sempre que o caráter urgente, quer de Instruções, quer de outros atos que por lei devam ser publicados, o justifique.

Para além do *Boletim Oficial*, o Banco de Portugal disponibiliza um *Manual de Instruções*, constituído pela totalidade das Instruções em vigor, consultável em Legislação e Normas – SIBAP.

O *Boletim Oficial* eletrónico contém:

- **Instruções**

  Atos regulamentares do Banco de Portugal designados por Instruções, numeradas sequencialmente dentro do ano a que respeitam, classificadas tematicamente.

- **Avisos do Banco de Portugal**

  Publicados em *Diário da República*.

- **Cartas Circulares**

  Emitidas pelo Banco de Portugal e que, apesar do seu conteúdo não normativo, se entende dever ser objeto de divulgação alargada.

- **Informações**

  Selecionadas e cujo conteúdo justifica a sua inclusão no Boletim, numa perspetiva de compilação e difusão mais generalizada, designadamente:

  – Comunicados do Banco de Portugal e do Banco Central Europeu;
  – Lista das Instituições de Crédito, Sociedades Financeiras, Instituições de Pagamento e Instituições de Moeda Eletrónica registadas no Banco de Portugal;
  – Seleção de referências e resumos de legislação nacional e comunitária respeitante a matérias que se relacionam com a atividade das Instituições sujeitas à supervisão do Banco de Portugal.

CARTAS CIRCULARES

BANCO DE PORTUGAL
EUROSISTEMA

Carta Circular n.º CC/2021/00000047

Assunto: Recomendações sobre Gestão da Continuidade de Negócio (revistas)

O Conselho Nacional de Supervisores Financeiros (CNSF) aprovou, no passado dia 20 de setembro de 2021, as Recomendações sobre Gestão da Continuidade de Negócio (revistas), que foram elaboradas, conjuntamente, pelo Banco de Portugal, pela Autoridade de Supervisão de Seguros e Fundos de Pensões e pela Comissão do Mercado de Valores Mobiliários, no âmbito da iniciativa do CNSF de *Better Regulation* para o setor financeiro.

As Recomendações consubstanciam um conjunto de requisitos mínimos que devem ser implementados e aprofundados pelas instituições de acordo com a natureza das suas atividades, dimensão e complexidade, modelo organizativo e perfil de risco, tendo em consideração o princípio da proporcionalidade. A sua publicação visa reforçar o conteúdo das orientações anteriormente emitidas sobre esta matéria e procura refletir a evolução que, entretanto, se registou na gestão da continuidade de negócio das instituições financeiras nacionais.

As Recomendações refletem o quadro legislativo e regulamentar vigente harmonizado a nível Europeu e os princípios internacionais mais relevantes sobre esta matéria, nomeadamente os princípios do Comité de Supervisão Bancária de Basileia sobre gestão do risco operacional e resiliência operacional.

Neste contexto, as Recomendações – disponibilizadas em Anexo - devem ser observadas pelas instituições de crédito, sociedades financeiras, instituições de pagamento e instituições de moeda eletrónica sujeitas à supervisão prudencial direta do Banco de Portugal.

Em particular, a observância das disposições constantes das Recomendações pode ser adaptada às especificidades de cada instituição, tendo em consideração o princípio da proporcionalidade. Em todo o caso, as Recomendações podem ser implementadas de forma flexível. Porém, nos casos em que sejam adotadas políticas ou procedimentos que não se afigurem condizentes com o quadro de orientações ora estabelecido, as instituições devem demonstrar às autoridades de supervisão a adequação das suas opções e que as soluções adotadas são apropriadas e oferecem, pelo menos, o mesmo grau de resiliência das enunciadas naquele documento.

Com a publicação destas Recomendações deixam de vigorar as anteriores Recomendações sobre GCN, de 2010, divulgadas pela "Carta-Circular[1] nº 75/2010/DSB" do Banco de Portugal, de 3 de dezembro de 2010.

[1] https://www.bportugal.pt/cartacircular/0752010dsb

Enviada a:
Instituições de Crédito, Empresas de Investimento, Sociedades Financeiras, Instituições de Pagamento e Instituições de Moeda Eletrónica.

Anexo I à Carta Circular n.º CC/2021/00000047

RECOMENDAÇÕES SOBRE
GESTÃO DA CONTINUIDADE DE NEGÓCIO
(revistas)

Índice

A. Introdução

A Gestão da Continuidade de Negócio ("GCN") é um requisito chave das organizações em todos os setores de atividade e, em particular, nos setores de atividades essenciais, como é o caso do setor financeiro. Assim, cabe às autoridades de supervisão competentes garantir que as instituições financeiras dispõem de planos de contingência e de continuidade de negócio que assegurem a capacidade para operarem numa base contínua e minimizarem perdas na eventualidade de uma perturbação grave da sua atividade.

Em face da forte inovação de base tecnológica e da progressiva automatização e digitalização dos processos operacionais, comerciais e de gestão das instituições financeiras, a GCN assume uma preponderância acrescida, em especial no que respeita à componente tecnológica. Tal como demonstrou a pandemia de Covid-19, que obrigou as instituições a adaptarem rapidamente o seu modo de interação, tanto com os clientes, como com os trabalhadores, as capacidades de GCN, nas vertentes operacional, humana e tecnológica, são absolutamente críticas para evitar disrupções na atividade desenvolvida. Por último, a GCN assume também um caráter essencial, no atual quadro económico, em que a resiliência e estabilidade das instituições que compõem o sistema financeiro se revestem de especial relevância para apoiar a retoma da atividade económica.

Neste contexto, o Conselho Nacional de Supervisores Financeiros ("CNSF") decidiu proceder à revisão das suas Recomendações às instituições financeiras sobre a GCN, emitidas em 2010, de modo a promover a sua atualização face às referências legislativas e regulamentares vigentes e às melhores práticas atuais.

Sendo esta uma matéria de importância transversal para a resiliência do setor financeiro, as presentes Recomendações, à semelhança das anteriores, foram elaboradas em conjunto pelo Banco de Portugal ("BdP"), a Autoridade de Supervisão de Seguros e Fundos de Pensões ("ASF") e a Comissão do Mercado de Valores Mobiliários ("CMVM") – doravante, "autoridades competentes" – sob a égide do CNSF, e no âmbito do projeto de "*Better Regulation*" do setor financeiro.

Aliás, as anteriores Recomendações previam já a possibilidade de o CNSF "*proceder à sua atualização ou adaptação, tendo em conta, quer a experiência entretanto recolhida junto das instituições, quer as alterações ao nível das condicionantes de risco a que as instituições possam estar sujeitas, e ainda outros desenvolvimentos que se venham a registar em relação a esta matéria.*".

Assim, as principais alterações destas Recomendações revistas face às Recomendações de 2010, são a seguir indicadas:

i. A introdução e clarificação de requisitos e expectativas de supervisão em conformidade com as alterações verificadas na regulamentação de referência nesta matéria, a nível europeu e internacional em geral, face ao enquadramento regulatório vigente em 2010, aquando da elaboração das recomendações anteriores. Em concreto, são introduzidos requisitos e expectativas de supervisão relativos ao governo interno das instituições, à subcontratação de serviços, processos ou funções de negócio críticos, e à supervisão do risco associado às tecnologias de informação e comunicação (TIC) e à segurança;

ii. Uma abordagem revista e adaptada aos principais riscos para a continuidade da atividade e segurança das instituições decorrente da crescente digitalização do sistema financeiro, que tem resultado na maior

utilização e dependência das instituições das TIC e de outras tecnologias inovadoras, alertando para procedimentos que garantam a cibersegurança e a resiliência operacional das instituições face a ataques externos, na ótica de deteção e prevenção de eventos disruptivos em complemento à capacidade de recuperação e resposta;

iii. A previsão de boas práticas apreendidas no contexto da pandemia de Covid-19, incluindo o reforço da relevância de os procedimentos de recuperação e resposta considerarem diferentes estratégias de recuperação adaptadas aos múltiplos cenários (por exemplo o recurso ao sistema de trabalho remoto - "teletrabalho"), e a necessidade de contemplar com adequada criticidade e para múltiplos cenários, igualmente, os procedimentos de reporte interno ao órgão de administração e externo ao supervisor, com adequada exatidão e tempestividade;

iv. A clarificação de alguns requisitos, com base nas lições aprendidas no âmbito do processo de supervisão, nomeadamente no que respeita ao planeamento da continuidade de negócio de instituições inseridas num grupo, à incorporação da continuidade de negócio no quadro de gestão de riscos das instituições e à consideração adequada dos riscos associados à subcontratação de processos e funções críticos.

As Recomendações refletem os princípios internacionais relevantes sobre esta matéria, em especial no âmbito da harmonização europeia da regulação financeira.

De forma transversal a todo o setor financeiro, releva a proposta de Regulamento do Parlamento Europeu e do Conselho relativo à resiliência operacional digital do setor financeiro ("DORA"[1]).

No que se refere ao setor segurador, ressegurador e de fundos de pensões, relevam também as seguintes Orientações[2] e Parecer da Autoridade Europeia dos Seguros e Pensões Complementares de Reforma (EIOPA, na sigla inglesa): Orientações relativas ao sistema de governação ("EIOPA-BoS-14/253"); Orientações sobre segurança e governação das tecnologias da informação e comunicação ("EIOPA-BoS-20/600"); Orientações relativas à subcontratação de prestadores de serviço de computação em nuvem ("EIOPA-BoS-20-002"); e "*Opinion on the supervision of the management of operational risks faced by IORP* ("EIOPA-BoS-19-247"). Relevam, ainda, a Diretiva 2009/138/CE, do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, relativa ao acesso à atividade de seguros e resseguros e ao seu exercício ("Solvência II") e o Regulamento Delegado (UE) 2015/35 da Comissão, de 10 de outubro de 2014, bem como a Diretiva (UE) 2016/2341, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2016, relativa às atividades e à supervisão das instituições de realização de planos de pensões profissionais (IRPPP).

No setor bancário, relevam, adicionalmente, as seguintes Orientações da Autoridade Bancária Europeia[2] (EBA, na sigla inglesa): Orientações relativas ao governo interno ("EBA/GL/2017/11"); Orientações relativas à subcontratação ("EBA/GL/2019/02"); e Orientações relativas à gestão do risco associado às TIC e à segurança ("EBA/GL/2019/04"). Relevam ainda a Diretiva 2013/36/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013 ("CRD-IV") e a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015 ("DSP2"), bem como os "*Principles for the Sound Management of Operational Risk*" ("BCBS195") e os "*Principles for Operational Resilience*" ("BCBSd509"), ambos do Comité de Supervisão Bancária de Basileia.

No setor dos mercados e instrumentos financeiros, relevam igualmente os "*High-level Principles for Business Continuity*", da Organização Internacional de Reguladores de Valores Mobiliários ("IOSCO FR32/2015")[2].

Em particular, as presentes Recomendações complementam, para efeitos do quadro legal e regulamentar nacional, o disposto no regime jurídico de acesso e exercício da atividade seguradora e resseguradora, aprovado pela Lei n.º 147/2015, de 9 de setembro, no regime jurídico da constituição e do funcionamento dos fundos de pensões e das entidades gestoras de fundos de pensões, aprovado pela Lei n.º 27/2020, de 23 de julho, nas

[1] Proposta de 24/09/2020.

[2] De notar que, nalguns casos, inexiste uma correspondência direta com o teor das Orientações ou dos Princípios, as quais serviram como ponto de referência para a revisão das Recomendações.

Normas Regulamentares da ASF n.os 14/2005-R[3], de 29 de novembro, e 8/2009-R, de 4 de junho; no Aviso n.º 3/2020 do Banco de Portugal; no Código dos Valores Mobiliários e no Regime Geral dos Organismos de Investimento Coletivo, onde se estabelece, essencialmente, a obrigatoriedade quanto à existência de um plano de continuidade de negócio.

Estas Recomendações consubstanciam um conjunto de requisitos mínimos que devem ser implementados e aprofundados pelas instituições de acordo com a natureza das suas atividades, dimensão e complexidade, modelo organizativo e perfil de risco, tendo em consideração o princípio da proporcionalidade. Em todo o caso, as Recomendações podem ser implementadas de forma flexível. Não obstante, as instituições devem ser capazes de demonstrar a adequação da adoção de soluções não condizentes com o quadro de orientações ora estabelecido, em especial, que as mesmas oferecem pelo menos o mesmo grau de resiliência daquelas que são previstas neste documento. Com efeito, as autoridades competentes acompanharão a adequação da implementação destas Recomendações pelas respetivas instituições supervisionadas por referência ao seu grau de observância, nomeadamente através de ações direcionadas ou outros procedimentos de supervisão. Adicionalmente, os membros do CNSF poderão igualmente avaliar o grau de observância das Recomendações, a fim de verificar a necessidade e pertinência de se proceder a uma nova atualização ou adaptação das mesmas.

Estas Recomendações foram submetidas a consulta pública, tendo a resposta recebida sido ponderada e os comentários acolhidos na versão final, nos termos enunciados no correspondente Relatório da Consulta Pública do CNSF n.º 1/2021.

Assim, o CNSF, no uso das suas competências ao abrigo da alínea *f)* do n.º 2 do artigo 2.º do Decreto-Lei n.º 228/2000, de 23 de setembro, estabelece o seguinte:

i. São adotadas as Recomendações sobre gestão da continuidade de negócio dirigidas às instituições financeiras sujeitas à supervisão das autoridades competentes;

ii. As instituições financeiras devem observar as disposições apresentadas nas Recomendações, que compreendem um conjunto de requisitos mínimos e traduzem as expetativas de supervisão gerais das autoridades competentes;

iii. As instituições financeiras devem aplicar estas Recomendações tendo em conta a natureza das suas atividades, dimensão e complexidade, modelo organizativo e perfil de risco;

iv. Com a publicação destas Recomendações deixam de vigorar as anteriores Recomendações sobre GCN, de 2010, divulgadas pela "Carta-Circular[4] nº 75/2010/DSB" do Banco de Portugal, de 3 de dezembro, e pela "Circular n.º 11/2010" da ASF, de 11 de novembro[5], bem como através de comunicação datada de 1 de dezembro de 2010 na página da CMVM na Internet[6].

[3] A ASF encontra-se atualmente a desenvolver trabalhos regulatórios com vista à emissão de uma nova norma regulamentar relativa ao sistema de governação das empresas de seguros e de resseguros.
[4] https://www.bportugal.pt/cartacircular/0752010dsb
[5] https://www.asf.com.pt/winlib/cgi/winlib.exe?skey=&cap=&pesq=7&thes0=14924&label=ESTRUTURAS+DE+GOVERNA%C3%87%C3%83O&doc=19711
[5] https://www.cmvm.pt/pt/Legislacao/Legislacaonacional/Recomendacoes/Pages/Recomendações-da-CMVM,-do-Banco-de-Portugal-e-do-ISP-sobre-Gestão-da-Continuidade-do-Negócio.aspx

B. Recomendações

1. Necessidade de políticas estruturadas para preservar a continuidade de negócio

RECOMENDAÇÃO 1 – Política de Gestão da Continuidade de Negócio

As instituições devem dispor de uma política de gestão da continuidade de negócio que reflita o seu perfil de risco e seja proporcional à natureza das suas atividades, à sua dimensão, complexidade e modelo organizativo.

Referências-chave: EBA GL/2017/11 Parágrafo 208; EBA GL/2019/04 Parágrafos 79 e 81; EIOPA-BoS-20/600 Orientações 2, 3, 4, 6, 19 e EIOPA-BoS-14/253 Orientação 8; EIOPA-BoS-19-247 Parecer; BCBS195 Princípio 11; BCBSd509 Princípios 1 e 7.

As instituições devem instituir políticas e procedimentos que procurem assegurar o funcionamento contínuo do seu negócio, a recuperação atempada no caso de ocorrência de eventos disruptivos e o retorno aos padrões normais de atividade. Os eventos disruptivos podem tomar a forma de catástrofes naturais, pandemias, atos de terrorismo, falhas nos sistemas informáticos, incêndios, inundações ou falhas graves de energia. Em suma, qualquer evento suscetível de perturbar o normal funcionamento da instituição (de ora em diante designados, por simplificação, como "desastres").

A gestão da continuidade de negócio (GCN) deve consubstanciar-se numa abordagem integrada e estruturada da instituição, ou, quando aplicável, do grupo financeiro, devendo integrar as políticas globais de gestão de risco. A necessidade de ser adotada uma abordagem integrada da GCN não invalida que possam ser delineados outros planos de atuação especificamente vocacionados para determinadas componentes (e.g. planos de evacuação de edifícios, planos de segurança). Nestes casos, deve ser assegurada a devida integração desses planos no âmbito da política global de gestão da continuidade de negócio.

As instituições devem delinear uma política de gestão da continuidade de negócio ("política de GCN") ajustada às suas especificidades, integrando-a no sistema de gestão de riscos da instituição, em concreto, no âmbito do risco operacional. Assim, a política de GCN deve refletir os principais riscos a que a instituição se encontra exposta e as vulnerabilidades inerentes ao seu negócio, estrutura organizativa, governo interno, características das infraestruturas físicas, implementação geográfica, entre outros.

A política de GCN deve, por isso, estar alinhada com a estratégia de GCN que, por sua vez, deve ser parte integrante da estratégia de negócio global da instituição. Concretamente, para além de prever a seleção dos processos e funções de negócio críticos, e a definição das prioridades, procedimentos e recursos (humanos e materiais) a mobilizar, a política de GCN deve refletir as condições em que o negócio é normalmente desenvolvido. A abrangência e o grau de detalhe na planificação para mitigar situações de desastre deve por isso ser proporcional à natureza da atividade da instituição, à sua dimensão e complexidade. Consequentemente, a política de GCN deve ser objeto de ajustamento contínuo ao desenvolvimento do negócio.

Esta política deve ser escrita, devidamente aprovada, e deve aplicar-se a todos os colaboradores relevantes, bem como, no que se afigure pertinente, aos prestadores de serviços da instituição. Adicionalmente, a política de GCN deve ser divulgada internamente a todos os colaboradores e disponibilizada, quando adequado, aos prestadores de serviços.

A política de GCN deve compreender a implementação de um processo de gestão da continuidade de negócio com diversas etapas, que abranjam, em particular, a definição de um plano de continuidade de negócio (PCN) que integre, por sua vez, uma análise de impacto no negócio de uma eventual interrupção não planeada da atividade (na sigla inglesa – BIA, "*Business Impact Analysis*") e a definição de uma estratégia ou plano de recuperação de desastres (na sigla inglesa – DRP, "*Disaster Recovery Plan*") que envolva as várias vertentes afetadas. Estes procedimentos de recuperação não devem circunscrever-se aos domínios da tecnologia, da informática ou das infraestruturas físicas, sendo essencial que se encontrem igualmente acautelados os métodos de recuperação funcional dos negócios, o que implica, nomeadamente, que sejam consideradas as vertentes de recursos humanos e a sua mobilidade e adaptabilidade. Adicionalmente, a política de GCN deverá prever a definição de uma política de comunicação para efeitos da GCN, a realização de testes, manutenção e auditoria ao PCN e ainda a formação de todos os colaboradores envolvidos e sensibilização a todos os níveis da instituição.

Por fim, no atual contexto da digitalização do setor financeiro - que induziu uma crescente dependência das instituições pelas tecnologias de informação e comunicação (TIC), tornando o respetivo negócio mais vulnerável a incidentes de segurança, incluindo ciberataques - importa que, para além das capacidades de gestão da continuidade e resposta e de recuperação, as instituições assegurem uma gestão adequada dos riscos em matéria de segurança das TIC a que estão expostas, por forma a prevenir e detetar potenciais disrupções da sua atividade desta natureza.

2. Estrutura de responsabilidades

RECOMENDAÇÃO 2 – Responsabilidades do órgão de administração

O órgão de administração das instituições deve garantir a salvaguarda da resiliência operacional da instituição.

Referências-chave: EBA GL/2019/04 Parágrafo 80; EIOPA-BoS-20/600 Orientações 2, 3, 4, 6, 7; IOSCO FR32/2015 Princípio 1; BCBS195 Princípio 11.

O órgão de administração de cada instituição financeira é responsável por promover a resiliência face a desastres e por assegurar o funcionamento contínuo da instituição, designadamente a recuperação célere do negócio em caso de perturbações na atividade. Nesse contexto, o órgão de administração deve considerar a GCN como parte integrante da gestão de riscos, articulando-a também com as políticas de controlo interno da instituição, sendo o responsável máximo pela implementação e desenvolvimento da política de GCN da instituição. Esta deve, por isso, ser objeto de aprovação pelo órgão de administração, ao qual compete também assegurar um acompanhamento próximo do processo de implementação e desenvolvimento e promover uma discussão regular sobre GCN nas suas reuniões.

A competência pela implementação da política de GCN pode ser delegada num comité criado para o efeito ou em outra unidade de estrutura ou responsável que se julgue adequado, o que não afasta, contudo, a responsabilidade última do órgão de administração. Para esse efeito, deverá ser designado, no seio do órgão de administração, um interlocutor para as matérias relacionadas com a GCN. Caso se justifique a criação de um comité ou outra unidade de estrutura, ou responsável, com a competência específica de implementar a política de continuidade de negócio, deve existir uma adequada atribuição e segregação de responsabilidades, devendo, em especial, ser mantida uma linha direta de reporte ao órgão de administração. No caso das instituições financeiras de maior dimensão e com um modelo de negócio mais complexo, esta unidade de estrutura deve dispor de recursos afetos em exclusividade, devendo ponderar-se a criação de uma função de continuidade de negócio. Esta função deve ter como principais responsabilidades: dar suporte ao órgão de administração na definição da política de GCN e monitorização da respetiva implementação; monitorizar e rever a implementação de procedimentos de continuidade de negócio,

reportando e aconselhando o órgão de administração, regularmente ou, quando se revele necessário, acerca da respetiva ativação; assegurar a adesão dos prestadores de serviços à política de GCN; e assegurar que todos os colaboradores têm conhecimento da política de GCN e demais procedimentos relacionados com a GCN.

Em caso de desastre, o órgão de administração deve ser o responsável pela ativação dos procedimentos de continuidade de negócio. Nesse sentido, o PCN da instituição deve prever canais de comunicação institucional que garantam que o órgão de administração é informado contínua e adequadamente acerca dos procedimentos executados em situação de contingência e do estado de recuperação de negócio.

O órgão de administração deve também promover e incentivar a sensibilização dos recursos humanos para a prevenção e preparação para eventuais situações de perturbação da atividade, o que pode ser conseguido através da atribuição clara de uma prioridade elevada à política de GCN, nomeadamente através da afetação, a esta política, de recursos humanos e financeiros em quantidade e qualidade suficientes para assegurar uma implementação abrangente e robusta.

RECOMENDAÇÃO 3 – Responsabilidades em caso de desastre

A política de GCN deve contemplar uma definição clara das responsabilidades em caso de desastre.

Referências-chave: EBA GL/2017/05 Parágrafo 54; EIOPA-BoS-20/600 Orientações 6, 15; IOSCO FR32/2015 princípio 2.

A política de GCN deve prever uma estrutura de responsabilidades, no âmbito da qual se defina expressamente, de forma clara e objetiva, a divisão de atribuições entre os colaboradores que participam na estratégia de recuperação, quando ativada em caso de desastre. Assim, os colaboradores da instituição devem compreender, inequivocamente, as funções que lhes estão atribuídas numa situação de emergência.

Em caso de necessidade de ativação do PCN, as instituições devem possuir uma equipa de colaboradores afetos, com tarefas e responsabilidades bem definidas, para atuar nesse caso. No âmbito desta estrutura de responsabilidades, deve ser estabelecida uma equipa/função com poderes de decisão e com ampla capacidade de intervenção (função de gestão de crises), a qual pode ter uma composição distinta do órgão de administração, em resultado da situação excecional em que é ativada. A esta equipa/função compete a decisão quanto às medidas tendentes à recuperação do negócio.

Os colaboradores que integram a referida estrutura de responsabilidades devem ser qualificados, devendo as instituições proporcionar-lhes um nível de formação específica adequada e continuamente atualizada. Em especial, os colaboradores devem estar completamente familiarizados com as infraestruturas alternativas que existam (cf. Recomendação 7), as quais devem estar totalmente operacionais e com os postos de trabalho alternativos preparados e plenamente disponíveis. A estrutura de organização interna das instituições deve dispor da identificação dos colaboradores com responsabilidades atribuídas, bem como da respetiva cadeia de substitutos para que, em caso de ativação do PCN, esta possa lidar eficazmente com qualquer situação de desastre razoavelmente previsível.

Assim, com vista a acautelar o risco de se verificar uma indisponibilidade de recursos humanos, o PCN deve prever regras de substituição claras, bem como regras de mitigação em caso de perda de colaboradores fundamentais para a continuidade da atividade da instituição em situação de desastre.

As instituições devem garantir que os colaboradores a quem estejam atribuídas responsabilidades na recuperação do negócio dispõem de toda a informação necessária para o exercício das funções que lhes estão atribuídas nesse contexto.

3. Processo de gestão da continuidade de negócio

RECOMENDAÇÃO 4 – Plano de Continuidade de Negócio

As instituições devem estabelecer e implementar um PCN no âmbito do processo de GCN, por forma a maximizar as capacidades de prestação de serviços numa base contínua e para limitar as perdas na eventualidade de uma perturbação grave da sua atividade.

Referências-chave: EBA GL/2017/11 Parágrafo 212, 213; EBA GL/2019/04 Parágrafos 77-82; EIOPA-BoS-20/600 Orientações 2, 8, 13, 15, 21 e 22 e EIOPA-BoS-14/253 Orientação 8; EIOPA-BoS-19-247 Parecer; BCBSd509 Princípio 3.

O PCN é uma componente essencial da política de GCN. O PCN constitui um plano de ação detalhado que estabelece as medidas e os procedimentos necessários para a recuperação da atividade nos níveis e tempos predefinidos, abrangendo os meios (documentos, procedimentos, instruções ou outros) que permitam à instituição gerir uma eventual interrupção não planeada da atividade, incluindo o processo de retorno, com a maior brevidade possível, a níveis de qualidade de serviço normais. No caso de grupos financeiros, o PCN deverá discriminar a relação entre a empresa-mãe e as subsidiárias/sucursais na gestão de crise.

O PCN deve consubstanciar a estratégia de recuperação delineada pela instituição, com base na análise do impacto no negócio. Deve estabelecer e atribuir tarefas e responsabilidades e delegar poderes em caso de uma interrupção não planeada da atividade, assim como definir os critérios que presidem à ativação do próprio plano. Estes critérios devem ter em consideração a potencial gravidade de um impacto na atividade da instituição em consonância com os objetivos de recuperação definidos na análise de impacto no negócio.

O PCN deve ser documentado, aprovado pelo órgão de administração e conter informação relativa à periodicidade da sua revisão, devendo ainda ter em consideração os riscos que possam ter um impacto negativo nas áreas de negócio, funções, processos e sistemas da instituição, em particular aqueles que são suportados por serviços de TIC. Como tal, o PCN deve também servir objetivos de proteção e/ou restabelecimento da confidencialidade, integridade e disponibilidade dos sistemas e serviços de TIC, bem como especificar as condições para a sua ativação nesses casos.

As instituições financeiras devem coordenar-se com as partes interessadas internas (e.g. todas as áreas de negócio) e externas (e.g. prestadores de serviços) e agentes intra-grupo (se aplicável) pertinentes, durante a elaboração do PCN.

O PCN deve, assim, estabelecer procedimentos e atribuir responsabilidades que, em caso de desastre, permitam:

- Registar todos os incidentes, avaliar os respetivos danos, dar resposta e resolvê-los, priorizando as ações de recuperação;
- Avaliar a necessidade de ativar o PCN, incluindo para assegurar a confidencialidade, integridade e a disponibilidade dos sistemas e serviços críticos TIC que dão suporte aos processos e às funções de negócio da instituição;
- Transferir o exercício dos processos e funções de negócio considerados críticos para uma infraestrutura alternativa ou, se necessário, ativar os procedimentos de trabalho remoto;
- Recuperar as funções de negócio e as infraestruturas tecnológicas de suporte de acordo com os níveis de serviço e os tempos predefinidos;
- Proceder ao retorno das operações no local habitual, quando este se encontrar disponível, ou em outro local que o venha a substituir.

Em concreto, para que o PCN seja eficiente e eficaz, deve identificar, no mínimo:

- A estrutura de responsabilidades de acordo com a política de GCN. Em concreto, os respetivos papéis, responsabilidades e autoridade para atuação em relação ao PCN (cf. Recomendação 3);
- O conjunto de colaboradores a convocar para garantir a continuidade de negócio da instituição em situação de contingência, incluindo os métodos que permitam estabelecer um contacto imediato com os substitutos, no caso de os primeiros estarem inacessíveis (cf. Recomendação 3);
- Uma análise de impacto no negócio com diferentes graus de severidade e em consonância com as diferentes áreas de negócio da instituição. Esta deverá levar à definição de objetivos de recuperação para cada processo da instituição (cf. Recomendação 5);
- Os processos e as funções de negócio críticos (cf. Recomendação 5);
- Os respetivos critérios de ativação que devem ter em consideração o resultado da análise do impacto no negócio (cf. Recomendação 5);
- As estratégias e os procedimentos de recuperação para cada uma dos processos e funções de negócio críticos, incluindo funções subcontratadas, bem como recuperação de ficheiros e documentação crítica (cf. Recomendações 6 e 8);
- As infraestruturas tecnológicas e os equipamentos necessários para a operação em situação de contingência (cf. Recomendação 6);
- Os procedimentos e as informações necessárias que permitam o retorno à atividade normal (cf. Recomendação 6);
- Os procedimentos e critérios específicos que cubram a possibilidade de ativação de infraestruturas alternativas (e.g. infraestruturas tecnológicas, Centro de Processamento de Dados (CPD) secundário ou deslocação do pessoal), incluindo procedimentos para ativação de trabalho remoto, caso as infraestruturas alternativas sejam também elas afetadas por um evento (e.g. pandemia de saúde pública) - (cf. Recomendação 7);
- Uma lista de contactos dos elementos que fazem parte da estrutura de responsabilidades definida na política de GCN (cf. Recomendação 9);
- Os planos de comunicação entre colaboradores da instituição, órgão de administração, agentes externos, prestadores de serviços e outras partes interessadas em situação de contingência (cf. Recomendação 9).

A instituição deve promover a divulgação do PCN a todas as áreas funcionais, geográficas e unidades de estrutura da mesma. Para tal, o PCN deverá ser facilmente acessível a todos os elementos envolvidos no processo de

recuperação. Em particular, para além da simples distribuição do PCN em suporte papel, deve ser implementado o recurso a plataformas informáticas de intranet ou Internet, de forma a permitir a consulta remota do documento, e ações de formação internas para uma maior familiarização dos colaboradores com o mesmo.

RECOMENDAÇÃO 5 – Análise do Impacto no Negócio

As instituições devem fundamentar o PCN num exercício analítico de avaliação de impactos para o negócio. Esta análise deve permitir identificar os processos e as funções de negócio críticos, os principais fatores dos quais depende a sua continuidade (internos e externos), assim como os níveis de proteção adequados perante diferentes cenários.

Referências-chave: EBA GL/2017/11 Parágrafo 211 e EBA GL/2019/04 Parágrafos 78 e 79; EIOPA-BoS-20/600 Orientações 4, 20, 21 e EIOPA-BoS-14/253 Orientação 8; IOSCO FR32/2015 Princípio 5; BCBSd509 Princípio 3.

Como parte de uma gestão sólida da continuidade de negócio as instituições devem realizar análises de impacto no negócio. Esta análise deve avaliar a exposição da instituição a perturbações graves no negócio e avaliar os seus potenciais impactos, quantitativa e qualitativamente, recorrendo, para o efeito, a dados internos e/ou externos e à análise de cenários, incluindo cenários extremos.

As instituições financeiras devem assegurar que os seus sistemas e serviços de TIC são concebidos e alinhados com a análise de impacto no negócio de modo a promover a continuidade e segurança destes sistemas.

A análise de impacto no negócio é, assim, uma das componentes essenciais do PCN e consiste em identificar:

- Os processos e as funções de negócio críticos para a instituição, ou seja, aqueles que, no caso de serem interrompidos, têm o potencial de gerar implicações mais significativas na continuidade da atividade, na reputação, na situação financeira e/ou nas contrapartes da instituição. Esta categorização de processos e funções de negócio críticos deve ser periodicamente atualizada;
- As infraestruturas que dão suporte a esses processos e funções de negócio críticos, em particular as de cariz tecnológico;
- A existência de dependências internas e externas relativamente a esses processos e funções de negócio críticos.

Consequentemente, a análise de impacto no negócio deve contemplar as seguintes fases:

- Identificação e classificação, em termos de criticidade, dos riscos suscetíveis de gerar uma interrupção da atividade e que possam originar um impacto material para a instituição (como por exemplo, os ataques cibernéticos);
- Identificação de cenários de interrupção plausíveis, incluindo estimativas das respetivas probabilidades de ocorrência e da duração provável dos seus efeitos. Não se afigurando razoável quantificar probabilidades de ocorrência, a análise deve procurar definir uma gradação qualitativa de probabilidades, o que permitirá identificar os cenários mais e menos prováveis. Para este efeito, as instituições devem considerar os riscos a que se encontram especialmente expostas (por exemplo, risco sísmico no caso dos edifícios que se encontram numa região de elevada atividade sísmica; risco de inundação, no caso de se encontrarem em regiões propensas a esses fenómenos);

- Definição de objetivos de recuperação em consonância com todas as áreas de negócio. Estes objetivos devem incluir uma predefinição do tempo máximo necessário até que um sistema, processo ou função seja reposto ("Recovery Time Objective" - RTO) e do período de tempo máximo durante o qual podem ser perdidos dados relativos a um determinado nível de serviço ("Recovery Point Objective" - RPO), após uma interrupção grave e não planeada da atividade. A instituição deve assegurar os meios necessários para dar resposta aos objetivos de recuperação definidos pela análise de impacto no negócio, através da sua estratégia de recuperação, consoante a criticidade dos processos definida pelas áreas de negócio, e não o contrário, i.e., os constrangimentos técnicos ou humanos não devem condicionar os objetivos de recuperação;
- Avaliação da continuidade de funcionamento de sistemas e serviços de TIC e de manutenção da segurança da informação;
- Cálculo do impacto da interrupção de processos e funções de negócio críticos sobre os clientes finais;
- Avaliação dos impactos financeiros, não financeiros (por exemplo, ao nível da confidencialidade, integridade e disponibilidade da informação), operacionais, legais e reputacionais da interrupção de processos e funções de negócio críticos, considerando períodos de tempo diversos.

As instituições devem, assim, ser capazes de caracterizar os cenários de acordo com o trinómio probabilidade/impacto/duração, o que permitirá que a estratégia de recuperação incida sobre os cenários mais relevantes para a instituição. A redundância de componentes críticas poderá ser crucial para assegurar a continuidade da atividade em caso de desastre.

A análise de impacto no negócio deve ser realizada com a participação das áreas de negócio relevantes, embora seja importante que todo o processo seja coordenado de forma centralizada e que, em especial, sejam definidos critérios uniformes para a identificação da importância crítica e consequente prioridade das funções e processos de negócio. Caso seja apropriado, devem também participar na análise de impacto no negócio prestadores de serviços e outros intervenientes externos relevantes. Os resultados da análise devem ser claramente documentados, comunicados ao órgão de administração e devem ser mantidos facilmente acessíveis.

A análise de impacto no negócio, incluindo os pressupostos que lhe estão subjacentes, deve ser revista periodicamente e, em particular, sempre que se verifiquem alterações relevantes ao nível operacional ou quando ocorram eventos externos que afetem significativamente a atividade da instituição, ou ainda em resultado das conclusões retiradas dos testes realizados.

RECOMENDAÇÃO 6 – Definição e implementação da Estratégia de Recuperação

As instituições devem definir e implementar uma estratégia de recuperação dos seus processos e funções de negócio que permita estabelecer os objetivos e as prioridades de recuperação tendo por base os resultados da análise de impacto no negócio.

Referências-chave: EBA GL/2017/11 Parágrafo 212 e EBA GL/2019/04 Parágrafo 83, 84, 85 e 86; EIOPA-BoS-20/600 Orientações 8, 10, 15, 21 e 22 e EIOPA-BoS-20-002 Orientação 7; IOSCO FR32/2015 Princípio 3; BCBSd509 Princípio 3 e 6.

As instituições, com base na análise de impacto no negócio e respetiva definição de processos e funções de negócio críticos, nos cenários plausíveis e nos objetivos de recuperação, devem elaborar estratégias de recuperação e resposta a desastres.

Com efeito, conforme as especificidades do negócio da instituição e a sua envolvente, pode ser identificada uma diversidade de acontecimentos que devem ser considerados na elaboração de cenários que tomem em consideração vários tipos de desastres. No entanto, pode ser legítimo que nem todos os cenários sejam contemplados pelo PCN, quer porque a instituição (e o seu órgão de administração) considera que os custos associados à implementação de planos de recuperação para determinados cenários são injustificáveis, quer porque se entenda que a probabilidade de ocorrência de certos cenários é despicienda. A identificação do que se encontra abrangido pelo PCN e do que se encontra excluído é determinante para que não se criem falsas expectativas quanto à resiliência da instituição.

A estratégia de recuperação deve centrar-se na recuperação das operações das áreas de negócio críticas, processos de apoio, ativos de informação e respetivas interdependências para evitar efeitos adversos no funcionamento das instituições e, consequentemente, no sistema financeiro.

A estratégia de recuperação deve especificar as ações necessárias para assegurar a continuidade e recuperação, em particular dos sistemas e serviços de TIC críticos, dentro dos objetivos de recuperação da instituição. Para este efeito, poderá ser criado um sistema de alerta que permita a deteção atempada de incidentes.

A estratégia de recuperação de desastres deve ser submetida a auditorias independentes. Entende-se, neste contexto, por auditorias independentes as ações de auditoria interna (incluindo com recurso a subcontratação) ou externa, cuja realização seja assegurada por elementos com independência organizacional das áreas diretamente envolvidas na definição e implementação da estratégia de recuperação de desastres, por forma a assegurar que a avaliação é realizada de forma imparcial e isenta. A estratégia de recuperação de desastres deve, igualmente, ser documentada e disponibilizada às unidades de negócio e de apoio da instituição, bem como ser facilmente acessível em caso de emergência. Por fim, a estratégia de recuperação deve ser testada e atualizada em consonância com as lições aprendidas com a realização de testes ou com a identificação de novos riscos e/ou ameaças.

Estratégia de recuperação para os processos e funções de negócio críticos

A estratégia de recuperação deve tomar em consideração a abrangência predefinida pela instituição. Assim, deve ser ponderado o desenvolvimento de planos de recuperação específicos para cada processo e função de negócio, de acordo com o tipo de cenários abrangidos pelo PCN. A estratégia de recuperação deve refletir a possibilidade de a indisponibilidade de recursos se prolongar no tempo, o que implicará que seja prevista a recuperação de diferentes níveis de serviço para diferentes tempos de indisponibilidade. Em concreto, pode ser definido um nível de serviço mais limitado para o primeiro momento de recuperação e planeada a forma de incrementar os níveis de serviço à medida que o tempo de indisponibilidade se prolonga. Os processos e funções de negócio com tempos de recuperação mais curtos devem, naturalmente, ser recuperados em primeiro lugar.

Atribuição de recursos aos processos e funções de negócio críticos

A instituição deve identificar os recursos necessários em situação de contingência, de modo a recuperar ou dar continuidade aos processos e funções de negócio críticos. A definição destes recursos deve ter por base cenários credíveis e proporcionados e refletir os níveis de serviço desejados. A atribuição de recursos deve seguir uma escala de prioridades assente nos tempos de recuperação.

Estratégia de recuperação para as infraestruturas tecnológicas

As infraestruturas tecnológicas são uma componente fundamental da estratégia de recuperação, sendo caracterizadas por uma elevada criticidade em caso de desastre. Assim, para cada uma das infraestruturas

tecnológicas que tenha sido definida como crítica, na sequência da avaliação dos processos e funções de negócio a que dão suporte, deve ser estabelecida a respetiva estratégia de recuperação.

A prestação de serviços de TIC é essencial às instituições. Neste sentido, as estratégias de recuperação devem tê-los em consideração, prevendo a implementação de medidas que garantam a continuidade de negócio independentemente da ocorrência de falhas de serviço por parte destes prestadores.

As instituições devem também dar elevada importância à definição dos processos de execução de cópias de segurança (*backup*) da informação e ao seu arquivo, que poderá passar pela duplicação do registo de informação em infraestrutura tecnológica e à recuperação de dados essenciais. Estes processos devem ainda definir qual a informação a salvaguardar, o local de armazenamento da informação e a frequência associada, considerando que os processos e funções críticos deverão ter naturalmente uma periodicidade mais curta.

As instituições devem ainda definir procedimentos de acessos lógicos à informação (nomeadamente, através da implementação de sistemas de controlo de acesso à informação), com vista não só à sua aplicação em caso de desastre, mas também como medida preventiva de proteção da confidencialidade, integridade e disponibilidade da informação crítica (incluindo dados pessoais). Estes procedimentos devem ser documentados, monitorizados e revistos periodicamente.

Procedimentos de cibersegurança

No atual contexto de crescente exposição a ataques cibernéticos, a cibersegurança assume particular importância como parte integrante da gestão global das TIC e dos riscos de segurança de uma instituição, com vista a assegurar a GCN. Assim, as instituições devem garantir que as medidas de segurança da informação aplicadas acautelam adequadamente os riscos cibernéticos, atendendo às características específicas de ataques deste tipo, designadamente:

- Os ataques cibernéticos são frequentemente mais difíceis de gerir (i.e., de identificar, detetar, responder e recuperar) do que a maioria das outras fontes de risco ligadas às TIC, sendo a extensão dos impactos, por vezes, igualmente difícil de determinar;
- Alguns ataques cibernéticos podem tornar ineficazes a gestão comum de riscos e os processos de continuidade de negócio, bem como os procedimentos de recuperação de desastres, uma vez que podem propagar *malware* aos sistemas de cópias de segurança a fim de os tornar indisponíveis;
- Os prestadores de serviços, intermediários e colaboradores em teletrabalho podem tornar-se canais de propagação de ataques cibernéticos. O acesso a redes de terceiros, via interligações ou qualquer outro meio, constitui uma ameaça silenciosa à propagação de ataques cibernéticos ao sistema de TIC da instituição. Por conseguinte, uma instituição interconectada, ainda que com pouca relevância individual, pode tornar-se vulnerável e uma fonte de propagação do risco, podendo resultar num impacto sistémico. Observando o princípio do elo mais fraco, a cibersegurança deve ser uma preocupação comum a todos os principais participantes no mercado e fornecedores de serviços críticos.

Neste contexto, ao efetivar a recuperação após um incidente, as instituições devem realizar verificações e reconciliações a fim de assegurar a integridade dos dados e a proteção dos dados pessoais. Além disso, as instituições devem procurar identificar e corrigir, de forma definitiva, as causas dos incidentes verificados. Por outro lado, as estratégias de recuperação devem ter em consideração opções alternativas para os casos em que

a recuperação possa não ser viável a curto prazo, devido aos custos, riscos e logística associados ou por força da ocorrência de circunstâncias imprevistas, ativando assim o recurso a infraestruturas alternativas.

RECOMENDAÇÃO 7 – Infraestruturas Alternativas

O processo de gestão da continuidade de negócio deve garantir a existência de infraestruturas alternativas, incluindo físicas, informáticas e de comunicações.

Referências-chave: EBA GL/2019/04 Parágrafo 79; EIOPA-BoS-20/600 Orientações 9, 20 e 22 e EIOPA-BoS-20-002 Orientação 3.

A existência de infraestruturas alternativas deve permitir a uma instituição garantir a continuidade dos seus processos e funções de negócio críticos (por exemplo, através da redundância operacional), ou a sua recuperação num período de tempo reduzido, no caso de uma situação de contingência provocar a inoperacionalidade das infraestruturas primárias ou impossibilitar o acesso a estas.

Por infraestruturas primárias entendem-se o local ou locais onde normalmente são executados os processos ou as funções de negócio críticos, abrangendo em simultâneo as infraestruturas de TIC e os postos de trabalho, assim como as redes de fornecimento que permitam a sua operacionalidade ou acesso a estas (e.g. telecomunicações, energia, água, transportes).

Uma instituição deve dispor de uma ou mais infraestruturas alternativas que lhe permitam fazer face a uma situação de contingência que possa provocar a inoperacionalidade da infraestrutura primária. Estas infraestruturas podem assumir diferentes graus de preparação:

- Infraestruturas que são mantidas atualizadas e preparadas para serem ocupadas a qualquer momento, mas que não são utilizadas para a operação diária ("hot sites");
- Infraestruturas que, não sendo utilizadas regularmente, estão disponíveis para a execução dos processos e funções de negócio críticos em caso de contingência, embora requerendo a sua ativação prévia ("cold sites");
- Infraestruturas que são utilizadas regularmente para determinado tipo de operações, mas que têm a capacidade de acomodar funções de negócio e recursos adicionais, caso um local de processamento principal fique inoperacional.

No entanto, caso tal situação seja inexequível, as instituições podem recorrer à subcontratação desse tipo de serviço a prestadores de serviços especializados, procurando a obtenção de direitos exclusivos para a utilização das infraestruturas alternativas contratadas. A título de exemplo, as instituições devem assegurar que os prestadores de serviços de TIC também mantêm, pelo menos, uma infraestrutura alternativa (e.g. um CPD alternativo), dotada de recursos, capacidades, funcionalidades e pessoal necessários e suficientes para assegurar a continuidade da atividade da instituição.

Em particular, as infraestruturas alternativas, consideradas na estratégia de recuperação de uma instituição, devem ser:

- Geograficamente localizadas a uma distância da infraestrutura principal que permita a exposição a um risco distinto, prevenindo que ambas sejam afetadas pelo mesmo evento;

- Capazes de assegurar a continuidade dos processos, funções de negócio e serviços de TIC críticos identificados na infraestrutura principal, permitindo cumprir os níveis de serviço necessários e suficientes para a operação dos mesmos dentro dos objetivos de recuperação. Neste sentido, é importante garantir que, por exemplo, o CPD secundário possua uma infraestrutura com uma capacidade não inferior ao CPD principal, quer em termos isolados para a instituição, quer no caso de um possível desastre que afete várias instituições em simultâneo que beneficiam da utilização das mesmas infraestruturas alternativas;
- Rapidamente acessíveis aos colaboradores da instituição para assegurar a continuidade do desempenho dos processos, funções de negócio e serviços críticos caso a infraestrutura principal se tenha tornado inacessível;
- Dependentes de redes distintas daquelas que servem as infraestruturas primárias (e.g. telecomunicações, energia, água, transportes);
- Devidamente testadas. Em particular, o CPD alternativo deve ser objeto de testes de capacidade a fim de garantir que este consegue dar uma resposta em caso de ativação. Na eventualidade deste serviço ser subcontratado, o prestador de serviços deve apresentar evidências de que o CPD secundário tem uma capacidade de resposta adequada.

Estas infraestruturas alternativas devem ainda ser periodicamente auditadas, de modo a garantir que os meios disponíveis se encontram permanentemente atualizados e adequados à atividade da instituição, sobretudo no caso em que sejam subcontratadas. Os procedimentos de ativação destas infraestruturas (em particular, as informáticas) devem garantir a sua segurança física e, em concreto, assegurar a segurança dos acessos físicos a estas infraestruturas de acordo com as tarefas e responsabilidades dos colaboradores da instituição. Estes procedimentos devem ser documentados e revistos.

Por fim, considerando a eventualidade de uma situação de desastre causar disrupções na infraestrutura principal e alternativa, ou causar disrupções que não afetem diretamente a infraestrutura, mas impeçam o acesso físico a esta, as instituições deverão estar dotadas de recursos, capacidades, funcionalidades e pessoal necessários e suficientes para assegurar a continuidade da respetiva atividade em regime de trabalho remoto ("teletrabalho"), nomeadamente em termos das capacidades TIC necessárias a este cenário. O regime de trabalho remoto poderá igualmente ser utilizado como forma de assegurar, pelo menos parcialmente, a existência de infraestruturas alternativas em determinados cenários de desastre.

RECOMENDAÇÃO 8 – Interdependências

A estratégia de recuperação deve tomar em consideração eventuais dependências, pelo que os pressupostos a utilizar quanto à disponibilidade e acesso aos serviços prestados por terceiros devem ser especialmente conservadores, devendo ainda ser previstas formas de mitigar estas dependências.

Referências-chave: EBA GL/2019/02 Parágrafos 49/59/104/107/112 e EBA GL/2019/04 Parágrafo 86; EIOPA-BoS-20/600 Orientações 21, 22 e 25 e EIOPA-BoS-20-002 Orientações 9, 10 e 12; EIOPA-BoS-19-247 Parecer; BCBSd509 Princípio 3 e 5.

Numa abordagem preventiva e mitigadora do risco de subcontratação, as instituições devem reconhecer nas suas políticas de GCN que os serviços ou infraestruturas subcontratados podem, também eles, sofrer disrupções ficando indisponíveis ou com níveis de serviço reduzidos. Neste sentido, uma componente crucial da política de GCN deve ser a descrição do tratamento dado a agentes externos e subcontratados em caso de desastre.

Assim, as instituições devem gerir as suas relações de dependência com terceiros, sejam estes agentes externos, prestadores de serviços ou agentes intra-grupo. O risco de dependência de entidades subcontratadas é

particularmente expressivo num cenário cujo evento subjacente afete várias instituições (desastres de grandes proporções), tendo em conta a pressão acrescida que resultaria sobre os prestadores de serviços de recuperação de negócio, dado que podem, eventualmente, não ter capacidade de responder ao volume exigido pelas instituições suas clientes. Num contexto de impossibilidade de dispor de infraestruturas alternativas próprias ou dedicadas, as instituições devem tomar as medidas necessárias para assegurar que os referidos prestadores de serviços são adequados face às suas características específicas (incluindo no domínio das TIC e ao nível da segurança da informação).

Estas medidas devem passar pelo conhecimento do prestador de serviços, nomeadamente através da solicitação pelas instituições de toda a informação relevante, incluindo o PCN do prestador de serviços, bem como testes e relatórios sobre medidas de continuidade da atividade, de modo a avaliar o grau de conforto que este lhes permite e a incorporar essa informação no PCN da própria instituição. Adicionalmente, devem ser previstos no PCN os mecanismos que assegurem a manutenção das relações com as entidades afetadas através das suas infraestruturas alternativas.

Por outro lado, as instituições devem assegurar, de forma permanente, que os acordos de subcontratação cumprem normas adequadas em matéria de desempenho e qualidade em consonância com as suas políticas. Compete, em especial, a cada instituição identificar claramente os deveres e responsabilidades das partes envolvidas, particularmente quando esteja em causa a subcontratação de funções essenciais ou importantes. Tal deve, nomeadamente, incluir as seguintes matérias:

- Níveis de serviço acordados para assegurar a continuidade da atividade da instituição. Para este efeito, as instituições devem assegurar-se que o prestador de serviços está dotado de um PCN adequado aos níveis de serviço subcontratados (na sigla inglesa – SLA, "Service Level Agreements"), de modo a que, mesmo perante cenários extremos, os SLA sejam cumpridos;
- Medidas de proteção da informação (e.g. controlo de acessos);
- Procedimentos de gestão de incidentes (e.g. definição de um modelo de cooperação em caso de ocorrência ou de suspeita de incidentes) e de reporte às instituições (e.g. apresentação de relatórios);
- Medidas de controlo do risco e condições para a ocorrência de subcontratação em cadeia. Neste âmbito, deve assegurar-se que o prestador de serviços permanece responsável perante as instituições, em situação de desastre ou de incumprimento dos níveis de serviço subcontratados, decorrente de disrupções que afetem os seus próprios prestadores de serviços.

As instituições devem ainda estabelecer cláusulas de saída nos seus contratos, assegurando que estão em condições de cessar os acordos de subcontratação sem qualquer interrupção indevida das suas atividades de negócio. A cessação do contrato não deverá limitar o cumprimento dos requisitos legais ou regulamentares aplicáveis ou prejudicar a continuidade e qualidade da prestação de serviços aos clientes.

Outros aspetos a ter em conta aquando da celebração de acordos de subcontratação são o potencial impacto da insolvência ou de outros incumprimentos dos prestadores de serviços e, se for caso disso, os riscos políticos existentes na jurisdição do prestador de serviços.

Em conformidade com o quadro jurídico aplicável neste âmbito, as instituições devem informar as autoridades competentes, de forma adequada e em tempo útil, de quaisquer alterações significativas e/ou acontecimentos

graves relativos aos acordos de subcontratação suscetíveis de terem um impacto significativo na continuidade das atividades de negócio.

Por fim, as instituições financeiras devem igualmente manter contactos entre si em matéria de GCN, mesmo em situação de normalidade, de modo a estimular a partilha de conhecimentos e experiências na matéria, com vista a auxiliar a sua prática e a ação em caso de eventual acionamento dos PCN.

RECOMENDAÇÃO 9 – Política de Comunicação

As instituições devem criar, manter, atualizar e testar, em articulação com as entidades relevantes, uma política de comunicação com todos os interessados, de modo a assegurar os fluxos de informação necessários à recuperação de processos e continuidade do negócio em caso de crise, assegurando as obrigações perante clientes e outras contrapartes, bem como o cumprimento de deveres de reporte às autoridades de supervisão.

Referências-chave: EBA GL/2019/04 Parágrafo 91; EIOPA-BoS-20/600 Orientações 15 e 24; IOSCO FR32/2015 Princípio 4/5; BCBSd509 Princípio 6.

No caso de uma interrupção ou emergência, e durante a implementação do PCN, as instituições devem assegurar que dispõem de medidas que garantam uma comunicação de informação eficaz, tempestiva e com elevados níveis de exatidão, a todas as partes interessadas: internas (entre colaboradores); externas (clientes, imprensa, etc.); autoridades competentes (em matéria de comunicação de desastres e de manutenção da comunicação dos reportes regulares de supervisão); e prestadores de serviços pertinentes (prestadores de serviços subcontratados, entidades pertencentes ao mesmo grupo ou prestadores de serviços terceiros). A política de comunicação deve, assim, servir os seguintes objetivos: assegurar a boa execução do PCN, minimizar os riscos reputacionais e manter a confiança do público e das autoridades.

Por forma a garantir a execução eficaz da política de comunicação, as instituições devem considerar, por exemplo:

- O recurso a formas de comunicação criadas especificamente para dar resposta às solicitações relacionadas com o desastre, tais como a criação de sítios na Internet e/ou linhas de atendimento telefónico dedicadas;
- Pelo menos no caso dos principais cenários identificados no âmbito da análise de impacto no negócio, a elaboração antecipada de minutas de comunicados de imprensa e documentos semelhantes, de modo a minimizar o tempo de reação e comunicação com o exterior, assim como o risco de erro ou de fuga de informação em situação de crise;
- A criação de listas de contactos para efeitos de comunicação interna, coligindo os contactos dos colaboradores relevantes para a recuperação de cada processo e função de negócio, em especial daqueles que integram a linha de comando (cf. Recomendação 4);
- A criação de listas de contactos, permanentemente atualizadas, dos interlocutores junto das entidades relevantes para a instituição em situação de desastre (por exemplo, autoridades de supervisão, outras instituições financeiras, nacionais ou estrangeiras, entidades gestoras de mercados regulamentados, órgãos de imprensa, etc.);
- As listas contemplando os interlocutores da própria instituição com as autoridades de supervisão devem ser transmitidas a essas autoridades.

As listas de contactos devem ter suporte informático e papel, com as cópias em localizações que garantam a sua integridade em quaisquer circunstâncias. Uma solução a considerar para as listas de contactos para efeitos de

comunicação interna poderá passar, consoante a dimensão da instituição e a complexidade da sua estrutura, pela disponibilização de cópias em papel transportáveis pelos colaboradores, recordando os pontos básicos do PCN, eventuais pontos de encontro e os contactos chave.

As instituições devem ainda procurar comunicar com outras instituições nacionais e estrangeiras, de forma a mitigar eventuais impactos sistémicos e transfronteiriços de incidentes de larga escala.

No que respeita à comunicação com as autoridades de supervisão, é fundamental que as instituições financeiras reportem todos os custos e perdas decorrentes de disrupções e incidentes operacionais, assim como lhes prestem informação, com elevados níveis de tempestividade e exatidão, acerca da ocorrência de qualquer desastre, incidente ou interrupção de funcionamento, emergência grave, falha nas TIC, potencial ou efetiva violação das informações dos clientes e/ou de atividade ilegal. A comunicação imediata às autoridades de supervisão de um incidente grave relacionado com a suspensão ou atraso de operações informáticas, incidentes financeiros relacionados com a manipulação de dados ou programas informáticos, e de falhas no sistema de processamento de informação, permite acautelar um eventual risco sistémico.

RECOMENDAÇÃO 10 – Testes e Manutenção do Plano de Continuidade de Negócio

As instituições devem assegurar a realização de testes, simulações, treinos e/ou outros procedimentos de preparação da ativação do PCN e de verificação da sua qualidade, em situações de risco mínimo a extremo, e a auditoria independente e atualização do PCN, pelo menos anualmente e sempre que necessário.

Referências-chave: EBA GL/2019/04 Parágrafo 87-90; EIOPA-BoS-20/600 Orientações 2, 5, 12, 13 e 23 e EIOPA-BoS-14/253 Orientação 8; IOSCO FR32/2015 Princípio 6; BCBS195 Princípio 11.

Testes, simulações e treinos

As instituições devem realizar testes, simulações, treinos e/ou outras medidas de preparação e verificação da qualidade e atualização do PCN. Estes testes devem demonstrar que as instituições conseguem manter a sua atividade até à recuperação da normalidade ou a níveis de serviço predefinidos. A frequência dos testes deve estar associada, por exemplo, à ocorrência de inovações/alterações tecnológicas ou decorrentes de incidentes de segurança informática.

Estas iniciativas podem ter diferentes amplitudes e níveis de abrangência, sendo expectável que as instituições complementem a realização de testes e treinos parcelares - que incidam sobre determinadas componentes do PCN - com testes mais abrangentes - que contemplem, em simultâneo, várias componentes do PCN. Em concreto, as instituições devem incluir no âmbito destes testes os processos, funções de negócio e serviços de TIC críticos. Além disso, devem ser realizados testes por referência aos vários cenários previstos no PCN, incluindo os cenários mais extremos. Em qualquer dos casos, as instituições devem incluir os prestadores de serviços em matéria de GCN referidos na Recomendação 8 *supra* (sobretudo no caso de processos e funções críticos e gestão da continuidade de negócio).

As instituições são responsáveis pela organização dos testes ao PCN, os quais devem ser executados de forma segura, incluindo por pessoas independentes e com conhecimentos suficientes em matéria de GCN. Entende-se, neste contexto, por pessoas independentes as que participam na realização dos testes e que não são diretamente responsáveis pela definição ou implementação do PCN, com vista a assegurar que os testes são conduzidos de forma adequada, com imparcialidade e isenção.

Os testes devem ser organizados com regularidade, esperando-se que as instituições de maior dimensão e complexidade realizem testes de maior amplitude com periodicidade, no mínimo, anual. Em todo o caso, devem ser promovidos, com maior regularidade, testes mais específicos e de âmbito mais delimitado.

Os resultados dos testes devem ser documentados e as insuficiências verificadas devem ser analisadas, resolvidas e reportadas ao órgão de administração.

Atualização e manutenção do PCN

O PCN deve ser revisto e atualizado no mínimo anualmente, embora possa ter de ser sujeito a revisões mais frequentes. Estas revisões devem ser realizadas em caso de ocorrência de eventos societários relevantes (e.g. reestruturações) e de alterações nas circunstâncias tecnológicas, de mercado ou regulamentares que o exijam.

As instituições devem igualmente rever o PCN caso se verifiquem alterações ao nível de processos e funções de negócio críticos, das listas de contactos, bem como na sequência da realização de testes ao PCN, de modo a corrigir as insuficiências apuradas. A atualização do PCN deve também ter em conta a experiência adquirida com a ocorrência de incidentes passados e contar, quando adequado, com a participação dos prestadores de serviços relevantes.

Auditoria do PCN

O PCN deve ser auditado por quadros internos da instituição ou através de mecanismos equivalentes que se adequem à dimensão, natureza e complexidade da sua atividade, sem prejuízo da realização de uma auditoria externa, caso a instituição a entenda importante nesta matéria. Estas revisões devem integrar o plano de auditorias plurianual da instituição, devendo, para o efeito, garantir-se a independência e a qualificação adequada dos auditores.

Esta revisão deve ser efetuada no mínimo anualmente, de acordo com um âmbito predefinido, e os seus resultados devem ser reportados ao órgão de administração. A periodicidade e o âmbito das auditorias devem ser proporcionais à relevância dos riscos identificados no contexto do processo de GCN.

Formação Interna

As instituições devem promover a realização de ações de formação que englobem todos os colaboradores (incluindo o órgão de administração) e, quando adequado, os prestadores de serviços relevantes, com vista a assegurar a respetiva preparação para o cumprimento dos seus deveres e responsabilidades, no âmbito do processo de GCN, bem como a recolher opiniões e contributos para a melhoria do PCN. As instituições devem manter evidências da realização destas ações de formação.

Além disso, as instituições devem promover a realização de ações de sensibilização em matéria de GCN para todos os colaboradores (incluindo o órgão de administração) e, quando adequado, para os prestadores de serviços relevantes.

3. Anexo

Tabela sumária de recomendações

RECOMENDAÇÃO 1 – Política de Gestão da Continuidade de Negócio

As instituições devem dispor de uma política de gestão da continuidade de negócio que reflita o seu perfil de risco e seja proporcional à natureza das suas atividades, à sua dimensão, complexidade e modelo organizativo.

RECOMENDAÇÃO 2 – Responsabilidades do órgão de administração

O órgão de administração das instituições deve garantir a salvaguarda da resiliência operacional da instituição.

RECOMENDAÇÃO 3 – Responsabilidades em caso de desastre

A política de GCN deve contemplar uma definição clara das responsabilidades em caso de desastre.

RECOMENDAÇÃO 4 – Plano de Continuidade de Negócio

As instituições devem estabelecer e implementar um PCN no âmbito do processo de GCN, por forma a maximizar as capacidades de prestação de serviços numa base contínua e para limitar as perdas na eventualidade de uma perturbação grave da sua atividade.

RECOMENDAÇÃO 5 – Análise do Impacto no Negócio

As instituições devem fundamentar o seu PCN num exercício analítico de avaliação de impactos para o negócio. Esta análise deve permitir identificar os processos e as funções de negócio críticos, os principais fatores dos quais depende a sua continuidade (internos e externos), assim como os níveis de proteção adequados perante diferentes cenários.

RECOMENDAÇÃO 6 – Definição e implementação da Estratégia de Recuperação

As instituições devem definir e implementar uma estratégia de recuperação dos seus processos e funções de negócio que permita estabelecer os objetivos e as prioridades de recuperação tendo por base os resultados da análise de impacto no negócio.

RECOMENDAÇÃO 7 – Infraestruturas alternativas

O processo de gestão da continuidade de negócio deve garantir a existência de infraestruturas alternativas, incluindo físicas, informáticas e de comunicações.

RECOMENDAÇÃO 8 – Interdependências

A estratégia de recuperação deve tomar em consideração eventuais dependências, pelo que os pressupostos a utilizar quanto à disponibilidade e acesso aos serviços prestados por terceiros devem ser especialmente conservadores, devendo ainda ser previstas formas de mitigar estas dependências.

RECOMENDAÇÃO 9 – Política de comunicação

As instituições devem criar, manter, atualizar e testar, em articulação com as entidades relevantes, uma política de comunicação com todos os interessados, de modo a assegurar os fluxos de informação necessários à recuperação de processos e continuidade do negócio em caso de crise, assegurando as obrigações perante clientes e outras contrapartes, bem como o cumprimento de deveres de reporte às autoridades de supervisão.

RECOMENDAÇÃO 10 – Testes e Manutenção do Plano de Continuidade de Negócio

As instituições devem assegurar a realização de testes, simulações, treinos e/ou outros procedimentos de preparação da ativação do PCN e de verificação da sua qualidade, em situações de risco mínimo a extremo, e a auditoria independente e atualização do PCN pelo menos anualmente e sempre que necessário.