Banco de Portugal

Carta-Circular nº 75/2010/DSB, de 3-12-2010

ASSUNTO: **Gestão da Continuidade de Negócio no sector financeiro - Recomendações prudenciais**

O Conselho Nacional de Supervisores Financeiros (CNSF) aprovou, no passado dia 9 de Setembro de 2010, as Recomendações sobre Gestão da Continuidade de Negócio no Sector Financeiro, que foram elaboradas, conjuntamente, pelo Banco de Portugal, pelo Instituto de Seguros de Portugal e pela Comissão do Mercado de Valores Mobiliários, no âmbito da iniciativa de Better Regulation.

As Recomendações consubstanciam um conjunto de boas práticas genéricas que o CNSF considera que devem ser implementadas e aprofundadas pelas instituições, de acordo com as respectivas características em termos de perfil de risco e tendo igualmente em consideração a natureza, a dimensão, a complexidade do negócio e o modelo organizativo de cada instituição. A sua publicação visa reforçar o conteúdo das orientações anteriormente emitidas sobre esta matéria pelas diferentes autoridades de supervisão e procura reflectir a evolução que entretanto se registou na gestão da continuidade de negócio das instituições financeiras nacionais. As Recomendações reflectem ainda aqueles que são considerados os princípios internacionais relevantes sobre esta matéria, em especial os "High-level principles for business continuity" estabelecidos, em Agosto de 2006, pelo "The Joint Forum", formado pelo Comité de Basileia sobre Supervisão Bancária, a Organização Internacional de Comissões de Valores Mobiliários (IOSCO) e a Associação Internacional de Supervisores de Seguros (IAIS).

Neste contexto, as Recomendações – disponibilizadas em Anexo - deverão passar a ser observadas pelas instituições de crédito, sociedades financeiras e instituições de pagamento sujeitas à supervisão do Banco de Portugal, nos termos que nelas se encontram estabelecidos (*cfr*. Secção "A. Introdução"). Em particular, a observância das disposições constantes das Recomendações pode ser adaptada às especificidades de cada instituição, em respeito do princípio da proporcionalidade. Além disso, reconhece-se que, neste domínio, não existem soluções universais, pelo que pode ser usada flexibilidade na implementação das Recomendações. Porém, nos casos em que sejam adoptadas 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 adoptadas são apropriadas e oferecem, pelo menos, o mesmo grau de resiliência daquelas que são enunciadas naquele documento.

Com a publicação destas Recomendações deixam de vigorar as Recomendações publicadas na Carta-Circular nº 100/2005/DSB de 26 de Agosto de 2005.

Enviada a:

Bancos, Caixa Central de Crédito Agrícola Mútuo, Caixa Económica Montepio Geral, Caixa Geral de Depósitos, Caixas de Crédito Agrícola Mútuo, Caixas Económicas, Instituições de Moeda Electrónica, Instituições Financeiras de Crédito, Sociedades de Factoring, Sociedades de Garantia Mútua, Sociedades de Investimento, Sociedades de Locação Financeira, Instituições de Pagamento, Agências de Câmbios, Sociedades Administradoras de Compras em Grupo, Sociedades Corretoras, Sociedades de Desenvolvimento Regional, Sociedades Emitentes ou Gestoras de Cartões de Crédito, Sociedades Financeiras de Corretagem, Sociedades Gestoras de Fundos de Investimento, Sociedades Gestoras de Fundos de Titularização de Créditos, Sociedades Gestoras de Patrimónios e Sociedades Mediadoras dos Mercados Monetário ou de Câmbios.

Banco de Portugal
EUROSISTEMA

CMVM

Instituto de Seguros de Portugal

RECOMENDAÇÕES SOBRE GESTÃO DA CONTINUIDADE DE NEGÓCIO

Índice

A. Introdução

A gestão da continuidade de negócio compreende o conjunto integrado de políticas e procedimentos que visam assegurar o funcionamento contínuo de uma organização, ou a recuperação atempada da sua actividade, no caso de ocorrência de eventos susceptíveis de perturbar o normal desenrolar do negócio, nomeadamente por implicarem a indisponibilidade das infra-estruturas físicas, dos sistemas informáticos ou dos recursos humanos, de forma isolada ou em simultâneo. Este tipo de eventos abrange, entre outros, cenários como catástrofes naturais, pandemias, actos de terrorismo, falhas nos sistemas informáticos, incêndios, inundações ou falhas graves de energia.

A gestão da continuidade de negócio contempla, assim, dois conceitos centrais, que se complementam: a continuidade operacional, que corresponde a uma situação em que a actividade é desempenhada sem interrupções ou com o mínimo de perturbações possível em termos de processos, pessoas, relações com parceiros e fornecedores, entre outros; e a recuperação, que visa assegurar o restabelecimento da actividade, nomeadamente após a verificação de um evento que provoque uma interrupção, completa ou parcial, do negócio ou que de algum modo impossibilite o seu desenrolar nos padrões habituais.

Tendo presentes os custos inerentes a um período de indisponibilidade – em especial no caso de uma instituição financeira –, bem como os riscos que daí decorrem, quer para a própria instituição, quer, possivelmente, para o resto do sistema financeiro, é essencial que a recuperação do negócio decorra no mais curto espaço de tempo ou mesmo, quando possível, que seja assegurada uma transição quase imediata para os modos alternativos de funcionamento. A gestão da continuidade de negócio reflecte o reconhecimento de que a única forma de assegurar esses objectivos passa pelo planeamento e pela adopção, com antecedência, de um conjunto de medidas de resposta a uma situação de perturbação da actividade.

Tal planeamento não pode deixar de ser realizado por referência à situação concreta de cada instituição e ao respectivo perfil de risco. Com efeito, as necessidades de cada instituição quanto ao modo como se processa a referida recuperação encontram-se intimamente relacionadas com aspectos como o seu modelo de negócio, a estrutura organizativa, as características das infra-estruturas físicas ou a implementação geográfica, entre outros. Neste contexto, a gestão da continuidade de negócio é um processo de natureza eminentemente idiossincrática, que não se coaduna com abordagens padronizadas.

Será esta em parte a justificação para que, internacionalmente, a gestão da continuidade de negócio não seja objecto de regulamentação específica, pelo menos sob a forma de requisitos vinculativos, sem prejuízo da existência, em Portugal e em outros Estados-membros da União Europeia, de um requisito genérico relativo à necessidade de implementação de uma política e/ou plano de continuidade de negócio (PCN), o qual é, em alguns casos, complementado por regulamentação ou recomendações.

Ainda assim, este é um tema que merece uma atenção particular dos supervisores financeiros e que justifica uma intervenção regulatória. Pese embora o facto de serem as próprias instituições as principais interessadas em assegurar a sua resiliência, sob pena de ser colocada em risco a própria sobrevivência, existem, neste domínio, evidentes externalidades, que importa acautelar. Desde logo, a resiliência das instituições financeiras constitui um elemento importante para a estabilidade financeira, pois não se encontrando salvaguardada a capacidade das instituições em resistir a choques de natureza operacional, não pode ser preservada a estabilidade do sistema financeiro, em caso de desastre. Além disso, mesmo no quotidiano, a percepção do público quanto à resiliência operacional das instituições

financeiras também pode contribuir para preservar a confiança no sistema, pelo que a gestão da continuidade de negócio concorre para os próprios objectivos das autoridades de supervisão, inclusive na ausência de desastres.

É neste contexto que se enquadra a emissão das presentes Recomendações, que resultam de uma iniciativa conjunta do Banco de Portugal (BdP), da Comissão do Mercado de Valores Mobiliários (CMVM) e do Instituto de Seguros de Portugal (ISP), no âmbito do Conselho Nacional de Supervisores Financeiros (CNSF), e que se integra no projecto de "*Better Regulation*" do sector financeiro.

O reconhecimento da importância em assegurar padrões mínimos de resiliência nas instituições financeiras já havia motivado a emissão de normativos regulamentares por parte de cada uma das autoridades, de forma autónoma. No entanto, entendeu-se que este é um domínio em que não se justifica a existência de quadros regulamentares diferenciados para os diferentes sectores do sistema financeiro e em que, pelo contrário, se verificam vantagens em ser definida uma abordagem integrada, dado tratar-se de uma área com fortes interdependências entre os vários intervenientes no sistema financeiro, a nível nacional e internacional.

As presentes Recomendações visam, assim, promover o desenvolvimento e/ou o aperfeiçoamento da função de continuidade de negócio a nível das instituições que operam no sistema financeiro português, tendo em vista o fortalecimento da sua capacidade de resposta a situações de perturbação da actividade.

Para esse efeito, é estabelecido um conjunto de Recomendações sobre gestão da continuidade de negócio. As Recomendações reforçam o conteúdo das orientações anteriormente emitidas sobre esta matéria pelos supervisores financeiros e procuram reflectir a evolução que entretanto se registou na gestão da continuidade de negócio das instituições financeiras nacionais, conforme verificado no âmbito da supervisão numa base contínua e em outras iniciativas *ad hoc*. As Recomendações reflectem ainda aqueles que são considerados os princípios internacionais relevantes sobre esta matéria, em especial os "*High-level principles for business continuity*" estabelecidos, em Agosto de 2006, pelo "*The Joint Forum*" [1], formado pelo Comité de Basileia[2], a Organização Internacional de Comissões de Valores Mobiliários[3] e a Associação Internacional de Supervisores de Seguros[4].

Esta iniciativa complementa o disposto no Aviso n.º 5/2008 do BdP[5], na Norma Regulamentar do ISP n. º 14/2005-R[6] e no Código dos Valores Mobiliários[7], onde se estabelece, essencialmente, a obrigatoriedade quanto à existência de um plano de continuidade de negócio.

---

[1] À data de elaboração destas Recomendações, o documento do "The Joint Forum" encontra-se disponível em http://www.bis.org/publ/joint17.htm.

[2] Basel Committee of Banking Supervision (BCBS).

[3] International Organisation of Securities Commissions (IOSCO).

[4] International Association of Insurance Supervisors (IAIS).

[5] Designadamente na alínea k) do n.º 2 do Artigo 15.º do Aviso do Banco de Portugal n.º 5/2008, de 1 de Julho, relativo aos sistemas de controlo interno das instituições de crédito e sociedades financeiras.

[6] Designadamente no n.º 10 do Artigo 8.º da Norma Regulamentar do Instituto de Seguros de Portugal n.º 14/2005-R, de 29 de Novembro, relativa aos "Princípios aplicáveis ao desenvolvimento dos sistemas de gestão de riscos e de controlo interno das empresas de seguros".

[7] Designadamente na alínea i) do n.º 1 do Artigo 305.º do CVM.

É importante esclarecer que o objecto destas Recomendações consiste, apenas, no planeamento para a continuidade operacional do negócio em caso de desastre, não abrangendo o conceito de gestão de crises financeiras. Em geral, uma crise financeira – embora configure igualmente uma circunstância excepcional, susceptível, porventura, de colocar em causa a sobrevivência da instituição – requer uma planificação de natureza distinta daquela que é exigida para as situações de desastre operacional. No entanto, existem, inevitavelmente, pontos de contacto entre estas duas componentes, não só porque uma situação de desastre pode acabar por implicar custos ou riscos financeiros de tal magnitude que acabe por evoluir para uma situação de dificuldades financeiras, como também porque existem elementos comuns em determinados aspectos estruturantes da planificação para situações de desastre e para situações de crise financeira. Nesse sentido, as políticas de gestão da continuidade de negócio e de gestão de crises financeiras compartilham determinados elementos, o que requer que seja salvaguardada a devida consistência entre ambas as componentes e que sejam consideradas as possibilidades de interacção entre elas; i.e. que, no âmbito da gestão da continuidade de negócio, sejam igualmente ponderadas as possíveis implicações financeiras de um desastre e, a partir daí, assegurada a interligação com a respectiva política de gestão de crises financeiras.

Não obstante a referida conexão, as presentes Recomendações incidem apenas na componente de gestão da continuidade de negócio e a temática da gestão de crises financeiras não é abrangida por estas Recomendações.

Esta iniciativa acomoda um dos dois pilares da gestão da continuidade de negócio no sistema financeiro, nomeadamente aquele que se refere à resiliência ao nível "micro". Para além da componente "micro", que compreende as iniciativas de gestão da continuidade de negócio a nível de cada uma das instituições financeiras, a resiliência do sistema financeiro requer também a implementação de medidas que reflictam uma abordagem "macro", ao abrigo da qual se adopta uma perspectiva integrada do sistema e se procura considerar as interdependências entre os diferentes agentes. Esta abordagem pressupõe uma perspectiva de conjunto que contemple, nomeadamente, as instituições financeiras, as próprias autoridades de supervisão, as infra-estruturas de pagamentos e as infra-estruturas de negociação, compensação, liquidação e contrapartes centrais, bem como os prestadores de serviços de informação sobre e aos mercados financeiros (e.g. Bloomberg, Reuters). A componente "macro" não constitui, portanto, objecto destas Recomendações, sem prejuízo da sua possível abordagem futura.

Estas Recomendações devem ser entendidas como um conjunto de boas práticas genéricas (*benchmarks*) que devem ser implementadas e aprofundadas pelas instituições, de acordo com as respectivas características em termos de perfil de risco e tendo igualmente em consideração a natureza, a dimensão, a complexidade do negócio e o modelo organizativo de cada instituição.

Por se entender que o tema da gestão de continuidade de negócio e as características específicas das várias instituições desaconselham a existência de requisitos tipificados, admite-se que a observância das disposições constantes das presentes Recomendações pode ser adaptada às especificidades de cada instituição, em respeito do princípio da proporcionalidade. Além disso, reconhece-se que, neste domínio, não existem soluções universais, pelo que pode ser usada flexibilidade na implementação destas Recomendações. Porém, nos casos em que sejam adoptadas políticas ou procedimentos que não se afigurem condizentes com o quadro de orientações ora estabelecido, as instituições devem ser capazes de demonstrar às autoridades de supervisão a adequação das suas opções e que as soluções adoptadas são apropriadas e oferecem, pelo menos, o mesmo grau de resiliência daquelas que são previstas neste documento.

As autoridades de supervisão continuarão a acompanhar, a nível de cada instituição, a adequação das respectivas abordagens para a gestão de continuidade de negócio, agora por referência ao grau de observância destas Recomendações.

Nesse âmbito, para além de ser respeitado o princípio da proporcionalidade e de ser adoptada uma abordagem flexível, a intensidade e a frequência da acção de supervisão pode também ser influenciada pela percepção das autoridades quanto às implicações, para a resiliência do conjunto do sistema financeiro, de uma eventual indisponibilidade de determinadas instituições ou áreas de negócio de uma instituição. As autoridades podem ainda adoptar determinados procedimentos de supervisão (e.g. ponderar a presença em simulacros ou testes conduzidos pelas instituições) ou discutir determinadas características da política de gestão da continuidade de negócio das instituições (e.g. os objectivos de recuperação) em função da referida percepção quanto ao papel das instituições para a resiliência do sistema financeiro.

Sem prejuízo de outras eventuais iniciativas relacionadas com a GCN, que incidam sobre uma ou mais instituições no âmbito dos respectivos processos de supervisão, o CNSF admite proceder a uma avaliação do grau de observância destas Recomendações pelas várias instituições, a fim de verificar a necessidade de se proceder à sua actualização 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.

B. Recomendações

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

RECOMENDAÇÃO 1

As instituições devem dispor de uma **política de gestão da continuidade de negócio** que reflicta o seu perfil de risco e seja proporcional à natureza das suas actividades e à sua dimensão e complexidade.

As instituições devem instituir políticas e procedimentos que procurem assegurar o funcionamento contínuo do negócio, ou a sua recuperação atempada, no caso de ocorrência de eventos susceptíveis de perturbar o seu normal desenrolar, tais como catástrofes naturais, pandemias, actos de terrorismo, falhas nos sistemas informáticos, incêndios, inundações ou falhas graves de energia (de ora em diante também designados, apenas por simplificação, como "desastres").

Tais políticas e procedimentos devem abranger a prevenção de desastres, a recuperação do negócio após interrupção provocada por um desastre, nos casos em que a prevenção não é suficiente, e o retorno aos padrões normais de actividade.

A gestão da continuidade de negócio deve consubstanciar-se numa abordagem integrada e estruturada, que abranja a instituição, ou grupo financeiro, na sua globalidade, e deve ser parte integrante das políticas globais de gestão de risco. O privilégio de uma abordagem integrada para a gestão da continuidade de negócio não invalida que possam ser delineados planos de actuação especificamente vocacionados para determinadas componentes (e.g. planos de evacuação de edifícios, planos de segurança); nestes casos, deve ser assegurada a devida integração dos planos no âmbito da política global de gestão da continuidade de negócio.

A política de gestão da continuidade de negócio deve ser ajustada às especificidades da instituição. Em particular, deve reflectir os principais riscos a que a instituição se encontra exposta e as vulnerabilidades inerentes ao seu negócio, à estrutura organizativa, às características das infra-estruturas físicas, à implementação geográfica, entre outros.

A abrangência ou o grau de detalhe e de profundidade na planificação para situações de desastre devem também ser proporcionados e reflectir a natureza da actividade da instituição, a sua dimensão e a sua complexidade.

As políticas e procedimentos de recuperação não devem circunscrever-se aos domínios da tecnologia, da informática ou das infra-estruturas físicas, sendo importante 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.

2. Estrutura de responsabilidades

RECOMENDAÇÃO 2

A salvaguarda da resiliência de uma instituição financeira constitui **responsabilidade do órgão de administração.**

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 actividade. Nesse contexto, o órgão de administração deve considerar a gestão da continuidade de negócio como constituindo parte integrante da gestão de risco, articulando-a também com as políticas de controlo interno da instituição, sendo os responsáveis máximos pela implementação e desenvolvimento da política de gestão da continuidade de negócio. Esta deve, por isso, ser objecto de aprovação em sede de 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 gestão da continuidade de negócio pode, contudo, ser delegada num comité criado para o efeito ou em outra unidade de estrutura ou responsável que se julgue adequada, o que não afasta, contudo, a responsabilidade principal 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 com a competência específica de implementar a política de continuidade de negócio, devem existir linhas de responsabilidade claras, devendo, em especial, ser mantida uma linha directa 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 afectos em exclusividade, devendo ponderar-se a criação de uma função de continuidade de negócio.

O órgão de administração deve ser o responsável pela activação dos procedimentos de continuidade de negócio, no caso de desastre.

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 actividade, o que pode ser conseguido através da atribuição clara de uma prioridade elevada à política da gestão da continuidade de negócio, nomeadamente através da afectação, a esta política, de recursos humanos e financeiros em quantidade e qualidade suficientes para assegurar uma implementação abrangente e robusta.

RECOMENDAÇÃO 3

A política de gestão da continuidade de negócio deve contemplar uma definição clara das responsabilidades em caso de desastre.

O PCN, a ser activado em caso de desastre, deve prever uma estrutura de responsabilidade clara, no âmbito da qual se defina expressamente a divisão de atribuições entre os colaboradores que participam na recuperação do negócio, de tal forma que estes compreendam, inequivocamente, as funções que

lhes estão atribuídas numa situação de emergência. Dado o risco de se verificar indisponibilidade de recursos humanos, o PCN deve ainda prever regras de substituição claras.

No âmbito desta estrutura de responsabilidade, deve ser estabelecida uma equipa com poderes de decisão e com ampla capacidade de intervenção, a qual pode ter uma composição distinta do órgão de administração, em resultado da situação excepcional em que é activada. A esta equipa deve competir a decisão quanto às medidas tendentes à recuperação do negócio.

O PCN deve ainda 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.

3. Processo de gestão da continuidade de negócio

RECOMENDAÇÃO 4

As instituições devem implementar um **processo de gestão da continuidade de negócio**, integrado nos seus processos de negócio, que compreenda, pelo menos, as etapas de análise do impacto no negócio, a definição de uma estratégia de recuperação e um plano de continuidade do negócio (PCN), assim como programas de testes, formação e sensibilização de todos os colaboradores, a todos os níveis da instituição.

O processo de gestão da continuidade de negócio deve estar integrado nos processos de negócio da instituição. Em particular, para além de ser necessário que a selecção das funções de negócio críticas traduza, efectivamente, as prioridades, os procedimentos a sistematizar e os recursos (humanos e materiais) a mobilizar, aquela deve também reflectir as condições em que o negócio é normalmente desenvolvido. Além disso, a política de continuidade de negócio deve ser objecto de ajustamento contínuo ao desenvolvimento do negócio.

Conforme detalhado de seguida, o processo de gestão da continuidade de negócio deve contemplar um conjunto de etapas bem definidas que abranjam, pelo menos, uma análise do impacto no negócio de uma eventual interrupção não planeada da actividade, a definição de uma estratégia de recuperação que envolva as várias vertentes afectadas e a definição de um plano de continuidade de negócio que consubstancie as etapas anteriores.

Adicionalmente, deverá ser definido um programa de testes e formação aos colaboradores envolvidos, bem como de sensibilização a todos os níveis da instituição, bem como devem ser tomadas iniciativas com vista à manutenção do plano.

3.1. Análise do impacto no negócio[8]

RECOMENDAÇÃO 5

[8] Equivale a "*Business Impact Analysis*" (BIA), na terminologia anglo-saxónica, que se generalizou.

As instituições devem fundamentar o seu processo de gestão da continuidade de negócio num exercício analítico de avaliação de impactos, para o negócio, de diferentes eventos (análise de impacto no negócio). Esta análise deve permitir identificar as funções de negócio críticas para a instituição, os principais factores dos quais depende a sua continuidade, tanto internos como externos, assim como os níveis de protecção adequados perante diferentes cenários.

A **análise do impacto no negócio** é a base do processo de gestão da continuidade de negócio e consiste em identificar:

- As funções de negócio críticas para a instituição, ou seja, aquelas que, no caso de serem interrompidas, têm o potencial de gerar implicações mais significativas na continuidade da actividade, na reputação, na situação financeira e/ou nas contrapartes da instituição;
- As infra-estruturas que dão suporte a essas funções de negócio críticas, em particular as de cariz tecnológico; e
- A existência de dependências internas e externas relativamente a essas funções de negócio.

A análise do impacto no negócio deve contemplar as seguintes fases:

- Identificação dos riscos susceptíveis de gerar uma interrupção da actividade e que possam originar um impacto material para a instituição;
- Identificação de cenários de interrupção plausíveis, incluindo estimativas das respectivas 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 actividade sísmica; risco de inundação, no caso de se encontrarem em regiões propensas a esses fenómenos);
- Estimativa do período de tempo durante o qual a instituição pode suportar a interrupção de cada uma das suas funções de negócio críticas;
- Cálculo do impacto da interrupção de funções de negócio críticas sobre os clientes finais; e
- Impacto financeiro, legal e reputacional da interrupção de funções de negócio críticas sobre a instituição, considerando períodos de tempo diversos.

Para efeitos da análise de impactos, pode ser mais apropriado que a análise incida sobre as consequências de determinados cenários e não na sua origem. A título de exemplo, a instituição pode estimar os impactos decorrentes de um cenário de derrocada de um dos seus edifícios, não se afigurando útil explicitar se tal consequência se deve a um sismo, a um atentado terrorista ou a um acidente de outra natureza. No entanto, a reflexão quanto à possível origem é importante para determinar a plausibilidade de cada cenário.

As instituições devem, assim, ser capazes de caracterizar os cenários de acordo com um trinómio probabilidade/impactos/duração, o que permitirá que a estratégias de recuperação incidam sobre os cenários mais relevantes para a instituição.

A análise do impacto no negócio, incluindo os pressupostos que lhe estão subjacentes, deve ser revista periodicamente e sempre que se verifiquem alterações relevantes ao nível operacional ou quando ocorram eventos externos que afectem significativamente a actividade da instituição.

A análise do 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 de negócio.

Os resultados da análise do impacto no negócio devem ser claramente documentados e ser mantidos facilmente acessíveis.

3.2. Definição da estratégia de recuperação

RECOMENDAÇÃO 6

As instituições devem definir uma estratégia de recuperação das suas funções de negócio que permita estabelecer os objectivos e as prioridades de recuperação das funções de negócio críticas tendo por base os resultados da análise de impacto no negócio.

A **estratégia de recuperação** deve passar, em primeiro lugar, pela definição dos objectivos quanto ao seu grau de abrangência, ou seja, pela clarificação dos cenários a que se pretende ser capaz de dar resposta. Com efeito, conforme as especificidades do negócio da instituição ou 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 pela política de gestão da continuidade de negócio, quer porque a instituição (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 daquilo que se encontra abrangido pelo PCN e daquilo que se encontra excluído é determinante para que não se criem falsas expectativas quanto à resiliência da instituição.

A definição da estratégia de recuperação deve ter por base os resultados da análise do impacto no negócio e deve traduzir-se na definição:

- De **objectivos de recuperação**, os quais constituem as metas predefinidas quanto à recuperação de funções de negócio críticas de acordo com um nível de serviço específico (nível de recuperação) dentro de um determinado período de tempo (tempo de recuperação), após uma interrupção grave e não planeada da actividade;
- De prioridades na **recuperação das funções de negócio críticas**, de acordo com o impacto potencial no desenvolvimento do negócio, na rendibilidade ou na reputação;
- De prioridades na **recuperação das infra-estruturas tecnológicas** que dão suporte às funções de negócio críticas.

As prioridades estabelecidas neste processo devem ainda orientar a atribuição de recursos (humanos ou outros) às funções de negócio críticas.

Objectivos de recuperação

Em caso de ocorrência de uma interrupção não planeada da actividade, e dependendo da gravidade da mesma, a instituição pode ser confrontada com escassez de recursos, pelo que é de esperar não ser possível recuperar todas as funções de negócio, nem recuperar os níveis de serviço habituais, mesmo para as funções passíveis de recuperação.

Em face dessa eventualidade, devem ser estabelecidos objectivos de recuperação, que permitam, no mínimo, recuperar de forma atempada as funções consideradas críticas.

Os objectivos de recuperação devem reflectir e ser proporcionais ao risco que cada função de negócio representa para a instituição e devem traduzir aqueles que a instituição considera serem os limites máximos aceitáveis de permanência da falha causada pela interrupção da actividade. A definição de objectivos de recuperação é determinante para que sejam estabelecidas prioridades de recuperação, de forma a que esta possa processar-se ordenadamente.

Estratégias de recuperação para as funções de negócio críticas

As estratégias de recuperação devem tomar em consideração a abrangência predefinida pela instituição.

Assim, podem ter que ser desenvolvidos diversos planos de recuperação para cada função de negócio, de acordo com o tipo de cenários abrangidos pela política de gestão de continuidade de negócio.

A estratégia de recuperação deve reflectir 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. As funções de negócio com tempos de recuperação mais curtos devem, naturalmente, ser recuperadas em primeiro lugar.

Estratégias de recuperação para as infra-estruturas tecnológicas

Para cada uma das infra-estruturas tecnológicas que tenha sido definida como crítica, na sequência da avaliação das funções de negócio a que dão suporte, deve ser estabelecida a respectiva estratégia de recuperação.

Devem ainda ser definidos processos de arquivo e recuperação (*backup*) de dados essenciais, incluindo informação detalhada sobre qual a informação a salvaguardar, o local de armazenamento da informação e a frequência associada, considerando que as funções críticas deverão ter naturalmente uma periodicidade mais curta.

Atribuição de recursos às funções de negócio críticas

A instituição deve identificar claramente quais são os recursos necessários em situação de contingência, de modo a recuperar ou dar continuidade às funções de negócio críticas.

A definição destes recursos deve ter por base cenários credíveis e proporcionados e reflectir os níveis de serviço desejados. A atribuição de recursos deve seguir uma escala de prioridades assente nos tempos de recuperação.

3.2.1. Infra-estruturas alternativas

RECOMENDAÇÃO 7

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

A existência de **infra-estruturas alternativas** deve permitir a uma instituição garantir a continuidade das suas funções de negócio críticas, ou a sua recuperação num espaço de tempo reduzido, no caso de uma situação de contingência provocar a inoperacionalidade das infra-estruturas primárias ou impossibilitar o acesso a estas.

Por infra-estruturas primárias entendem-se o local ou locais onde normalmente são executadas as funções de negócio críticas, abrangendo em simultâneo as infra-estruturas de tecnologias de informação 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).

Em relação às **infra-estruturas físicas alternativas**, estas podem assumir graus de preparação diversos, incluindo:

- Infra-estruturas que são mantidas actualizadas e preparadas para serem ocupadas a qualquer momento, mas que não são utilizadas para a operação diária ("*hot sites*");
- Infra-estruturas que, não sendo utilizadas no dia-a-dia, estão disponíveis para a execução das funções de negócio críticas em caso de contingência, embora requerendo a sua activação prévia ("*cold sites*");
- Infra-estruturas que são utilizadas no dia-a-dia 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.

As infra-estruturas físicas alternativas devem ser dotadas de todos os meios materiais, técnicos e informáticos necessários para assegurar a continuidade do desempenho, pelos colaboradores seleccionados, das funções de negócio críticas que tenham sido previamente identificadas.

Estas infra-estruturas devem ser alvo de inspecções periódicas pelas instituições, de modo a garantir-se que os meios disponíveis se encontram permanentemente actualizados e adequados à actividade da instituição.

As infra-estruturas físicas alternativas devem estar localizadas a uma distância que minimize a probabilidade de virem a ser também afectadas pelos riscos que afectam a infra-estrutura física primária. Para este efeito, deve ser privilegiado o critério do perfil de risco, de acordo com o qual as localizações devem, mais do que estar fisicamente distantes, apresentar perfis de risco diferentes, dado que é possível que as distâncias entre estas infra-estruturas não sejam suficientes para assegurar que o mesmo evento não as afecte simultaneamente.

No que respeita às **infra-estruturas informáticas alternativas**, deve ser garantida uma salvaguarda de dados com uma periodicidade que esteja de acordo com os tempos de recuperação previamente definidos. A situação ideal para suporte às funções de negócio críticas é, no entanto, a redundância operacional, de acordo com a qual são sistematicamente salvaguardados os dados informáticos que resultam da actividade contínua da instituição.

As infra-estruturas alternativas devem, na medida do possível, depender de redes de distintas daquelas que servem as infra-estruturas primárias (e.g. telecomunicações, energia, água, transportes).

Uma instituição deve dispor de uma ou mais infra-estrutura alternativas que lhe permitam fazer face a uma situação de contingência que possa provocar a inoperacionalidade da infra-estrutura primária. No entanto, caso tal situação seja inexequível, pode recorrer à subcontratação desse tipo de serviço a prestadores de serviços especializados, procurando a obtenção de direitos exclusivos para a utilização das infra-estruturas alternativas contratadas.

3.2.2. Interdependências

RECOMENDAÇÃO 8

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.

Num cenário de desastre, é de esperar que não se cumpram os pressupostos que seriam assumidos numa situação de normalidade. A consideração das circunstâncias excepcionais em que irá operar a instituição implica, por exemplo, o reconhecimento de que os serviços ou as infra-estruturas de que a instituição se encontra dependente poderão estar, também elas, indisponíveis ou com níveis de serviço reduzidos.

Assim, o PCN deve prever, por exemplo, meios de comunicação, fontes de energia ou de abastecimento de água alternativos ou soluções para a deslocação de colaboradores, no caso de ruptura dos meios de transporte habituais.

A avaliação da disponibilidade do fornecimento dos serviços ou dos recursos prestados ou disponibilizados por terceiros deve passar também pelo conhecimento dos planos de contingência dos fornecedores, pelo que as instituições devem solicitar às entidades de quem estão de alguma forma dependentes, informações sobre as suas próprias estratégias de recuperação, de modo a avaliar o grau de conforto que estes lhes permitem e 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 afectadas através das suas infra-estruturas alternativas.

As instituições financeiras devem igualmente manter contactos regulares entre si em matéria de gestão da continuidade de negócio, mesmo em situação de normalidade, de modo a estimular a partilha de conhecimentos e experiências na matéria, que auxiliarão a sua prática e a acção em caso de eventual accionamento dos PCN.

É especialmente importante que a instituição seja capaz de acautelar os riscos relacionados com os serviços prestados por entidades subcontratadas para efeitos de recuperação de processos, designadamente prestadores de serviços informáticos e locadores de espaços de trabalho alternativos. Para o efeito, compete a cada instituição assegurar-se de que, ao celebrar contratos desta natureza, são clarificadas as circunstâncias gerais e particulares em que a prestação de serviços deve ocorrer (e.g. contratação de postos de trabalho dedicados *vs*. postos de trabalho partilhados). Inclusivamente, a instituição pode preferir optar por celebrar contratos apenas com instituições que tenham também um PCN.

O risco de dependência de entidades subcontratadas é particularmente expressivo num cenário cujo evento subjacente afectasse várias instituições (catástrofes de grandes proporções). Em tal cenário, ocorreria uma pressão sobre os prestadores de serviços de recuperação de negócio, que poderiam eventualmente não ter capacidade de responder ao volume exigido pelas instituições suas clientes.

Na impossibilidade de disporem de infra-estruturas alternativas próprias ou dedicadas, a instituição deve tomar todas as medidas necessárias para assegurar que os referidos prestadores de serviços são os mais adequados face às suas características específicas. Estas medidas devem incluir, designadamente, um estudo da entidade a contratar, bem como o acompanhamento do contrato uma vez celebrado, garantindo que não existe degradação do nível de serviço nem saturação do prestador de serviço da qual pudesse resultar prejudicada a continuidade do negócio em situação de crise.

As instituições podem comunicar entre si de modo a avaliar a qualidade e a manutenção da qualidade dos serviços prestados e a prestar pelas entidades referidas, bem como realizar simulações "micro" e "macro", tal como descritas na Recomendação 11 infra, relativa à manutenção do PCN, de modo a acautelar para todo o mercado a boa qualidade dos serviços acessórios de recuperação de processos e gestão da continuidade de negócio.

3.2.3. Política de comunicação

RECOMENDAÇÃO 9

As instituições devem criar, manter, actualizar 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 os deveres para com as autoridades de supervisão, designadamente em matéria de reporte.

A política de comunicação para efeitos de gestão da continuidade de negócio deve contemplar a comunicação interna, intermédia e com o exterior, tendo em vista os seguintes objectivos: assegurar a boa execução do PCN, minimizar os riscos reputacionais e manter a confiança do público.

A **comunicação interna** respeita à comunicação dentro da própria instituição (entre colaboradores de todos os níveis); a **comunicação com o exterior** corresponde à comunicação com outras instituições, com as autoridades de supervisão, com os clientes, com a imprensa ou com o público em geral; e a **comunicação intermédia** compreende a comunicação da instituição com as famílias dos seus colaboradores em caso de ocorrência de uma situação de catástrofe, designadamente se tal situação

puder acarretar riscos para a integridade física dos colaboradores ou implicar a sua deslocação sem que estes possam comunicar directamente com as famílias.

Para garantir uma execução eficaz da política de comunicação, a instituição deve 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 *sites* 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 reacção 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 função de negócio, em especial daqueles que integram a linha de comando (*vide* igualmente Recomendação 10);
- A criação de listas de contactos coligindo os elementos de contactos dos interlocutores junto das entidades relevantes para a instituição (por exemplo, autoridades de supervisão, outras instituições financeiras, nacionais ou estrangeiras, entidades gestores de mercados regulamentados, órgãos de imprensa, etc.);
- A criação de listas organizadas dos interlocutores nomeados na própria instituição para servirem de ponto de contacto com o exterior em situação de catástrofe. As listas contemplando os interlocutores da própria instituição com as autoridades de supervisão devem ser-lhes transmitidas e manter-se actualizadas.

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.

3.3. Plano de Continuidade de Negócio

RECOMENDAÇÃO 10

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 actividade, assim como definir os critérios que presidem à activação do próprio plano.

O PCN constitui um plano de acção detalhado que estabelece as medidas e os procedimentos necessários para a recuperação da actividade nos níveis e nos tempos predefinidos, devendo, abranger os meios (documentos, procedimentos, instruções ou outros) que permitam à instituição gerir uma

eventual interrupção não planeada da actividade, incluindo o processo de retorno, com a maior brevidade possível, a níveis de qualidade de serviço normais.

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

- Avaliar os danos;
- Tomar uma decisão sobre a necessidade ou não de activar o PCN;
- Transferir as funções de negócio ou os centros de processamento de dados para um centro alternativo (caso exista);
- Recuperar as funções de negócio e as infra-estruturas tecnológicas de suporte de acordo com os níveis de serviço e os tempos predefinidos; e
- 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 incluir, no mínimo:

- Identificação clara da estrutura de coordenação das questões relacionadas com a gestão da continuidade do negócio, incluindo os respectivos papéis, responsabilidades e autoridades para actuação em relação ao PCN;
- Identificação das funções de negócio críticas;
- Indicação das estratégias de recuperação para cada uma das funções de negócio críticas, incluindo os respectivos níveis de recuperação e tempos de recuperação;
- Identificação das infra-estruturas, tecnologias de informação e comunicação e equipamentos necessários para a operação em situação de contingência;
- Lista de contactos de todos os elementos que fazem parte da estrutura de coordenação da política de gestão de continuidade de negócio;
- Conjunto de critérios a tomar em consideração para uma eventual activação do PCN, que tenham em conta, pelo menos, a potencial gravidade do impacto na actividade da instituição e os objectivos de recuperação previamente definidos;
- Procedimentos e critérios específicos que cubram a possibilidade de activação do centro de processamento alternativo, incluindo procedimentos para deslocação do pessoal;
- Identificação do conjunto de colaboradores a convocar para operar em situação de contingência, incluindo os respectivos contactos fora-de-horas;
- Procedimentos para a convocatória dos colaboradores designados para operar em situação de contingência, incluindo métodos que permitam estabelecer contacto imediato com os substitutos, no caso dos primeiros estarem inacessíveis;
- Procedimentos e outra informação que permitam restabelecer as funções de negócio críticas e/ou de operação em contingência, incluindo as que sejam desempenhadas por entidades subcontratadas;
- Procedimentos e outra informação que permitam activar as infra-estruturas tecnológicas e outras que sejam necessárias para o restabelecimento das funções de negócio críticas;

- Contactos dos vários fornecedores (de equipamento, *software* e outros), assim como detalhes sobre os contratos e condições especiais de fornecimento em situação de contingência;
- Procedimentos e outra informação que permitam recuperar ficheiros e documentação crítica;
- Plano de comunicação com os colaboradores da instituição e outras partes interessadas; e
- Procedimentos e outra informação que permitam o retorno à actividade normal.

O PCN da instituição deve estar claramente documentado e deve ser facilmente acessível a todos os elementos envolvidos no processo de recuperação e retorno. Para esse efeito, devem ser ponderadas soluções que permitam o acesso remoto ao PCN (e.g. via rede informática), salvaguardada a devida segurança e confidencialidade dos dados.

Do PCN deve ainda constar informação relativa à sua manutenção e à periodicidade da realização de testes e/ou simulações.

A instituição deve promover a divulgação interna do PCN e assegurar-se da familiarização dos seus colaboradores com o PCN. Esta divulgação deve ter lugar de modo transversal, cobrindo todas as áreas funcionais, geográficas e hierarquias da instituição.

Todos os colaboradores da instituição devem ter acesso à informação necessária para salvaguardar a sua integridade física em situação de desastre. Por outro lado, aos elementos a quem estejam atribuídas responsabilidades na recuperação do negócio deve ser facultado o acesso a toda a informação necessária para o exercício das funções que lhes estão atribuídas nesse contexto.

Devem ser utilizados os meios de divulgação interna que melhor se adequem à estrutura da instituição e aos métodos de trabalho, desde que assegurem os objectivos de ampla divulgação descritos supra. Em particular, deve ser ponderado, para além da simples distribuição do PCN em suporte papel, o recurso a plataformas informáticas de intranet ou internet, e acções de formação internas.

3.4. Testes e manutenção do PCN

RECOMENDAÇÃO 11

As instituições devem assegurar a realização de testes, simulações, treinos e/ou outros procedimentos de preparação da activação do PCN e de verificação da sua qualidade e actualização, em situações de risco mínimo a extremo, devendo o PCN ser auditado internamente e actualizado numa base mínima anual.

Testes, simulações e treinos

As instituições devem conduzir testes, simulações, treinos e/ou outros métodos e medidas de preparação e verificação da qualidade e actualização do PCN.

Estas iniciativas podem ter diferentes amplitudes e níveis de abrangência, sendo de esperar que as instituições complementem a realização de testes e treinos parcelares e que incidem sobre determinadas componentes do PCN, com testes mais abrangentes, que contemplem, em simultâneo, várias componentes do PCN.

Além disso, devem ser realizados testes por referência aos vários cenários previstos no PCN, incluindo aos cenários mais extremos.

As instituições são responsáveis pela organização de testes e simulações sobre os seus próprios planos, sendo no entanto aconselhável a realização progressiva (mas não exclusiva) de simulações ao nível "macro" (todo o mercado, incluindo os restantes agentes de mercado nacionais e eventualmente não nacionais).

Em qualquer dos casos ("micro" ou "macro"), as instituições devem procurar incluir nos testes os fornecedores e entidades subcontratadas relevantes, desde logo aqueles que prestem serviços em matéria de gestão da continuidade de negócio (e.g. serviços de informação, comunicação e locais alternativos), como referido na Recomendação 8 supra, relativa às interdependências.

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 (por exemplo, podem ser realizados, com maior frequência, testes às listas de contactos fora-de-horas).

Actualização e manutenção do PCN

O PCN deve ser revisto e actualizado no mínimo anualmente, embora possa ter de ser sujeito a revisões mais frequentes, no caso de ocorrência de eventos societários relevantes (e.g. reestruturações) ou de alterações nas circunstâncias tecnológicas, de mercado ou regulamentares que o exijam, bem como no que respeita a determinadas funções consideradas críticas pelo órgão de administração da instituição e às listas de contactos.

O PCN deve ainda ser sujeito a uma revisão por parte dos auditores internos da instituição ou através de mecanismos equivalentes que se adeqúem à dimensão, natureza e complexidade da sua actividade, sem prejuízo de auditoria externa, caso a instituição a entenda importante nesta matéria. Esta revisão deve ser efectuada no mínimo anualmente, de acordo com um âmbito predefinido, e os seus resultados devem ser reportados ao órgão de administração.

Como referido na Recomendação 10, a instituição deverá promover a familiarização dos colaboradores com o PCN, pelo que é importante que, para além da sua simples divulgação, sejam organizadas acções de formação interna dos colaboradores, com vista também à recolha de opiniões e contributos para melhoria do PCN.

Os prestadores de serviços relevantes à instituição (sobretudo no caso de funções críticas e gestão da continuidade de negócio) deverão participar nos exercícios de simulação e, quando adequado, na actualização do PCN e nas formações internas referidas supra.