INSTITUTO POLITÉCNICO DE LISBOA
INSTITUTO SUPERIOR DE CONTABILIDADE
E ADMINISTRAÇÃO DE LISBOA

AUDITORIA A PLANOS DE CONTINUIDADE DE NEGÓCIO NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO

Diogo Manuel Faustino Bruno

Lisboa, março de 2021

INSTITUTO POLITÉCNICO DE LISBOA

INSTITUTO SUPERIOR DE CONTABILIDADE E ADMINISTRAÇÃO DE LISBOA

AUDITORIA A PLANOS DE CONTINUIDADE DE NEGÓCIO NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO

Diogo Bruno

Dissertação submetida ao Instituto Superior de Contabilidade e Administração de Lisboa para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Auditoria, realizada sob a orientação científica do Professor Doutor Fernando J L Rodrigues.

Constituição do Júri:

Presidente _____ Prof. Especialista Gabriel Alves

Arguente_____ Prof.ª Especialista Ana Marinho Pires

Vogal_____ Prof. Doutor Fernando Rodrigues

Lisboa, março de 2021

AGRADECIMENTOS

Ao Professor Doutor Fernando Rodrigues por toda a ajuda e ensinamentos no decorrer do mestrado e por ter aceite ser orientador deste trabalho, sem o qual este não teria sido possível de realizar.

A todos os restantes professores que fizeram parte deste percurso letivo, que motivaram e encorajaram a que mais esta etapa fosse concluída.

A todos os colegas do Mestrado com quem foi partilhada esta experiência e que certamente tiveram o seu papel em tornar possível chegar a esta fase dos estudos, em particular à Margarida Costa pela entreajuda e disponibilidade no desenvolvimento do presente trabalho.

Aos meus colegas de trabalho e chefia, pelo incentivo dado ao longo de todo este tempo, pela compreensão e disponibilidade de ajudar na realização deste trabalho.

Aos meus Pais, Irmãos, Amigos e restante família por me terem apoiado a cumprir mais este objetivo.

À minha namorada Cristiana Serrano por toda a compreensão, apoio, ajuda e incentivo na concretização deste trabalho.

A todos fica o meu Agradecimento.

RESUMO

Com o avanço tecnológico como uma constante da nossa realidade, a forte dependência das tecnologias por parte das organizações é cada vez mais um fator que influencia as decisões. Desta forma surgem novas preocupações diretamente relacionadas com os Sistemas de Informação (SI) no âmbito da gestão de risco, controlo interno, segurança, entre outras áreas.

A dependência dos SI implica que estes sejam vistos como partes essenciais de muitos dos processos das organizações e as suas eventuais falhas, como situações críticas para a continuidade do negócio. Para garantir a resiliência da organização como um todo, importa que existam medidas bem definidas e testadas, que visem a recuperação do negócio em caso de desastre e não menos importante, a continuidade das operações vitais com as condições mínimas, nos momentos imediatos após os eventos disruptivos.

Um bom Plano de Recuperação de Desastre (PRD) em sintonia com Planos de Continuidade de Negócio (PCN) são fatores críticos de sucesso em organizações com um nível de maturidade elevado, que demonstram perante os seus Stakeholders a capacidade de ultrapassar adversidades garantindo a continuidade e viabilidade dos seus serviços/produtos.

A auditoria a PCN visa atestar que os procedimentos definidos são adequados à estrutura da organização, com meios suficientes para a sua execução a qualquer momento. A auditoria tem um papel determinante neste domínio confirmando a existência de testes e a conformidade entre os resultados e o que foi planeado numa fase inicial.

Com o objetivo de reunir um conjunto das melhores práticas de Continuidade de Negócio e que deverão ser objeto de auditoria, a presente investigação aborda diversos conceitos neste âmbito de forma a sustentar através da análise e revisão bibliográfica, o trabalho empírico que visa esclarecer se estas práticas são de facto tidas como relevantes e aplicadas por profissionais com experiencia em Continuidade de Negócio.

Palavras Chave: Auditoria; Planos de Continuidade de Negócio; Resiliência; Sistemas de Informação.

ABSTRACT

With technological advance as a constant of our reality, the strong dependence on technologies on the part of organizations is increasingly a factor that influences decisions. Thus, new concerns directly related to Information Systems (IS) arise in the areas of risk management, internal control, security, among other areas.

Dependence on IS implies that they are essential parts of many organizations processes and their eventual failures critical situations for business continuity. To guarantee the resilience of the organization as a whole, it is important that well defined and tested measures are in place, aimed at the recovery of the business in case of disaster and not less important, the continuity of vital operations with minimum conditions, in the immediate moments after disruptive events.

A good Disaster Recovery Plan (DRP) in line with Business Continuity Plans (BCP) are critical success factors in organizations with a high level of maturity, which demonstrates to Stakeholders the ability to overcome adversities ensuring the continuity and viability of their services/products.

The BCP audit aims to attest that the defined procedures are adequate to the structure of the organization, with sufficient means for their execution at any time. The audit plays a determining role in this area, it also confirms the existence of tests and compliance between results and what was planned at an early stage.

With the objective of sharing some of the best practices on Business Continuity that should be Audited, this investigation addresses some of the most important definitions so that through the bibliographic analysis and review it is possible to support the field work that tries to find if this practice is considered relevant and are applied by professionals with Business Continuity experience.

Keywords: Audit; Business Continuity Plans; Resilience; Information Systems.

Índice

Índice de Figuras

Lista de Abreviaturas

BCI – *Business Continuity Institute*

BCM – *Business Continuity Management*

BCMS – *Business Continuity Management System*

BCP – *Business Continuity Plan*

BIA – Business Impact Analysis

DRII – *Disaster Recovery Intitute International*

DRJ – *Disaster Recovery Journal*

GCN – Gestão de Continuidade de Negócio

PCN – Planos de Continuidade de Negócio

PDCA – *Plan-Do-Check-Act*

PRD – Plano de Recuperação de Desastre

RPO - *Recovery Point Objective*

RTO - *Recovery Time Objective*

SGCN – Sistema de Gestão de Continuidade de Negócio

SI – Sistemas de Informação

TI – Tecnologias de Informação

WRT - *Work Recovery Time*

1 INTRODUÇÃO

No âmbito do Mestrado em Auditoria o tema escolhido para a presente dissertação foi sobre Planos de Continuidade de Negócio, tratando-se de uma matéria auditável e por isso uma possibilidade neste contexto.

As principais motivações para a escolha do tema foram a inovação do mesmo aliada à importância que representa para as organizações em termos de resiliência e capacidade de subsistir face a eventos disruptivos que afetem negativamente a capacidade de desempenhar as suas funções básicas dentro da normalidade.

Com este trabalho pretende-se reunir um conjunto de práticas tidas como bons exemplos para a elaboração e manutenção de Sistemas de Gestão de Continuidade de Negócio robustos e capazes de dar resposta às necessidades das empresas neste sentido.

Pretende-se ainda com este trabalho e no âmbito do tema geral do Mestrado, estabelecer a relação entre o tema escolhido e a atividade de Auditoria, demonstrando o papel que esta desempenha e a importância que tem na garantia e controlo de que as melhores práticas estão a ser aplicadas nas organizações auditadas.

Para cumprir com o objetivo é proposta uma revisão bibliográfica das principais fontes sobre Continuidade de Negócio de forma a que sejam reunidos os principais conceitos sobre o tema, bem como as melhores práticas recomendadas pelas diversas fontes.

A presente dissertação apresenta conceitos como os de Sistemas de Gestão de Continuidade de Negócio, Planos de Continuidade de Negócio e Planos de Recuperação de Desastre bem como diversas práticas recomendadas para a elaboração destes. São abordados assuntos como a existência de seguros com cobertura de perdas relacionadas com a interrupção da atividade das organizações e certificações no âmbito da continuidade de negócio. É ainda estabelecida a relação e a importância que a atividade de Auditoria tem na Continuidade de Negócio.

De forma a ser possível aproximar o trabalho teórico com a realidade empresarial e profissional, serão desenvolvidos contactos com profissionais com experiencia nestas matérias através da realização de entrevistas e da distribuição de questionários de forma a que estes possam adicionar ao trabalho uma visão da realidade sobre o tema, podendo assim ser feita a análise comparativa entre a recolha bibliográfica e o que se pratica no tecido empresarial dando assim força à investigação feita.

2 SISTEMAS DE GESTÃO DE CONTINUIDADE NEGÓCIO (SGCN)

2.1 Definir SGCN

De acordo com o *IT Governance* (2019, fevereiro), os Sistemas de Gestão de Continuidade de Negócio (SGCN), tratam a capacidade de lidar com os diversos cenários de interrupção, dispondo de planos de contingência e recursos que possam satisfazer os requisitos exigidos pelos processos definidos nestes planos, de acordo com os objetivos da organização. Estes planos devem ser devidamente documentados e atualizados, por uma equipa competente e responsável pela resposta a eventos disruptivos e recuperação.

Os SGCN não poderão nunca deixar de ser realizados em conformidade com a realidade de cada organização. A CMVM, Banco de Portugal e ISP (Atual ASF) (2010, p.2) indicam que «as necessidades de cada instituição quanto ao modo como se processa a referida recuperação encontram-se intimamente relacionadas com aspetos como o seu modelo de negócio, a estrutura organizativa, as características das infraestruturas físicas ou a implementação geográfica». Embora este seja um documento especificamente direcionado a instituições do setor financeiro e segurador, os conceitos de continuidade de negócio serão transversais a outros setores e poderão servir de exemplo e de fonte de conhecimento destas matérias.

Desta forma, fica definido que esta gestão será especifica para cada organização e as suas características, não havendo, portanto, modelos padrão que possam ser aplicados de uma forma genérica, sendo nos detalhes que os planos se mostram mais adequados.

Neste documento de recomendações referido pela CMVM *et al.* (2010, p2) é justificada a ausência de regulamentação especifica sob a forma vinculativa a nível da continuidade de negócio, pelo facto destas matérias serem intimamente relacionadas com a situação concreta de cada instituição, observando-se, «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» sendo este complementado apenas por regulamentações ou recomendações.

Todavia, o documento também refere que «nos casos em que sejam adotadas 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 adotadas são apropriadas e oferecem, pelo menos, o mesmo grau de resiliência daquelas que são previstas neste documento» (CMVM et al, 2010, p.4).

Fica deste modo estabelecido que, embora não exista regulamentação vinculativa, as recomendações devem ser cumpridas e os desvios que possam existir devem ser devidamente justificados, sendo as autoridades de supervisão responsáveis por verificar a adequação das medidas de gestão de continuidade de negócio.

O Regulamento (UE) 2016/679 ao enquadrar a proteção das pessoas singulares no que concerne ao tratamento de dados pessoais e à sua livre circulação, conhecido como Regulamento Geral sobre a Proteção de Dados (RGPD) indica no artigo 32º que, quanto à segurança do tratamento, o responsável pelo tratamento e o subcontratante devem assegurar um nível de segurança adequado ao risco incluindo «[a] capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico», bem como, «um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.»

2.2 Caraterísticas dos SGCN

Considerando as recomendações da CMVM *et al.* (2010) podemos enumerar algumas das principais características para uma efetiva gestão de continuidade de negócio. Destacam-se:

- Dispor de políticas que reflitam um perfil de risco e que sejam proporcionais à natureza das suas atividades, bem como, à sua dimensão e complexidade;
- Assegurar que é da responsabilidade do órgão de administração a salvaguarda da resiliência da organização;
- Integrar nas políticas uma definição clara das responsabilidades em caso de desastre;
- Passar a incluir nos seus processos de negócio, as etapas de análise do impacto no negócio, a definição de uma estratégia de recuperação e Planos de Continuidade do Negócio (PCN), assim como, programas de testes, treino, formação e sensibilização de todos os colaboradores, aos vários níveis da organização;
- Fundamentar os processos de negócio com base nas análises de impacto, conhecidas por *Business Impact Analysis* (BIA's);
- Definir uma estratégia de recuperação com o apoio das áreas funcionais, alinhamento de objetivos e prioridades, tendo por base as BIA's;
- Garantir a existência de infraestruturas físicas, informáticas e comunicações alternativas;
- Ter em conta as dependências de terceiros no processo de recuperação e contemplar medidas que visem mitigar esta dependência;
- Criar e assegurar a manutenção, atualização e testes, em articulação com entidades relevantes, através de uma política de comunicação que garanta os fluxos de informação necessários para a recuperação de PCN, assegurando as obrigações perante terceiros;
- Relevar no PCN na atribuição de tarefas, responsabilidades e poderes em caso de interrupção da atividade, bem como, definir os critérios que levam à sua ativação;
- Assegurar que as organizações façam a realização de testes, simulações, treinos ou outros métodos de preparação, verificando a qualidade e atualização do PCN em situações de risco mínimo a extremo, devendo o PCN ser auditado e atualizado no mínimo anualmente.

Embora o documento referido anteriormente seja especificamente direcionado ao setor financeiro, banca e seguros, as recomendações são na sua generalidade abstratas o suficiente para que se pudessem aplicar a uma organização de outro setor. Na prática, todas a recomendações poderiam ser aplicadas por outro tipo de organizações à exceção dos pontos que são direcionados a características especificas da banca ou seguros.

Um ponto importante para tornar robusto um SGCN é o mapeamento dos processos da organização uma vez que «possibilita identificar, entender e compreender todos os processos produtivos de uma organização de modo a determinar os seus pontos fortes e fracos» (Manoel S.S. 2019, p.91).

Num documento sobre liderança num período em que todo o mundo foi afetado pela pandemia do coronavírus (COVID-19), por Buehler, Conjeaud, Giudici, Samandari, Serino *et al* (2020, p.2), artigo publicado pela *McKinsey* & *Company* é referido que:

> *[b]anks around the globe will play a critical role in this as systemic stabilizer for their customers, their employees, and for their economies at large. Cash and deposit services, credit extension, payment facilitation, and market making are all essential services.*

Para que os bancos possam ser considerados uma parte importante e com um papel critico na estabilização do sistema, é preciso que estes tenham resiliência suficiente para continuar a desempenhar as suas funções face a acontecimentos disruptivos como o caso do COVID-19.

Para que outras organizações se revejam e tenham confiança que os bancos possam representar este papel, é preciso acreditarem que as medidas de gestão de continuidade de negócio implementadas no setor estão preparadas para este tipo de eventos.

Desta forma podemos considerar que as recomendações das medidas de continuidade de negócio do setor bancário e segurador poderão servir de exemplo para outros setores, em que a GCN não seja uma preocupação tão presente na estratégia dessas empresas e cuja ausência em termos macroeconómicos tenha um impacto económico negativo em tempos disruptivos.

Um dos fatores determinantes da GCN é a amplitude das possibilidades colocadas na formação da estratégia dos planos. De acordo com a CMVM *et al* (2010, p.6):

> [a]s políticas e procedimentos de recuperação não devem circunscrever-se aos domínios da tecnologia, da informática ou das infraestruturas 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.

Esta mobilidade dos colaboradores pode ser um trabalho estrutural não considerado muitas vezes, como a capacidade de os colaboradores desempenharem diversas funções dentro da organização, ou terem formações mais técnicas sobre o funcionamento de equipamentos além daquilo que são as funções habituais.

Tomando por exemplo as consequências no mercado de trabalho que a pandemia do COVID-19 trouxe para todo o mundo nos finais de 2019 e ao longo de 2020, em que houve a necessidade de um reforço dos sistemas nacionais de saúde em termos operacionais, é importante por exemplo a capacidade de médicos desempenharem funções que habitualmente são da responsabilidade de enfermeiros ou outros de profissionais de saúde. No caso de empresas especializadas em recursos humanos e recrutamento, que tenham a saúde como uma parte do negócio e que numa situação de crise como anteriormente referida, considerem que esta área de negócio está a ter um aumento extraordinário, enquanto outras áreas setoriais sofrem um efeito contrário, será importante ter profissionais capacitados de serem canalizados para as funções que são ao momento as mais requisitadas.

2.3 Conhecer a Organização

De forma a planear e colocar em execução um SGCN, é preciso conhecer a organização a vários níveis, num trabalho com elevado nível de confiança de adequação à organização.

As questões enumeradas em seguida, de acordo Manoel S.S (2019, p.92), são questões que também em trabalhos de auditoria serão importantes para os auditores conhecerem a organização e deverão estar documentadas como base para a elaboração das medidas de continuidade de negócio. De acordo com o autor, as questões são as seguintes:

- Qual é o principal mercado onde a organização atua?
- Como é desenvolvido e comercializado o produto ou o serviço que a organização vende?
- Quais são os serviços, os produtos, os projetos que a organização entrega?
- Conhecem-se todos os departamentos e/ou áreas funcionais da organização?
- Existe um organograma publicado?
- Conhecem-se os clientes e o público-alvo da organização?
- Conhecem-se todas as localizações físicas (nacionais, internacionais) da organização?
- Quem são os seus principais prestadores de serviços, parceiros e fornecedores e que tipo de serviços são fornecidos por estas partes interessadas?

Ao estarem respondidas de forma completa as questões anteriormente listadas, será possível ter um conhecimento alargado da organização e possibilitar assim o início dos trabalhos.

2.4 Motivações para a existência de políticas de um SGCN

É importante fazer com que as políticas de GCN sejam tidas como fundamentais para as organizações. Neste enquadramento, devem ser claras as motivações para a elaboração destas mesmas políticas como podemos ver na Figura 2.1.

Nem sempre os decisores de topo de uma organização veem vantagens no investimento num SGCN, podendo não encontrar à primeira vista um evidente retorno neste investimento.

Manoel S.S (2019, p.42) utiliza o seguro automóvel como termo de comparação com um SGCN, indicando que este último funcionará como uma espécie de seguro para a organização na eventualidade de um desastre.

Partindo deste termo de comparação, será que existem (ou não) pessoas ou entidades coletivas, que na eventualidade da não existência da obrigatoriedade de fazer um seguro automóvel, não o fariam, como uma forma de poupança imediata, acreditando que não iriam mesmo precisar? Nesto caso, estarão as organizações que não têm políticas de continuidade de negócio a correr um risco de forma consciente?

Figura 2.1 *Motivações para Gestão de Continuidade de Negócio*

Fonte *Manoel, S.S (2019 p.31)*

2.5 Responsabilidade da Administração

A gestão de topo deve estar comprometida e envolvida com os objetivos e planos das políticas de continuidade de negócio, demonstrando liderança, fornecendo recursos e efetuando as devidas revisões. Uma possibilidade é a criação de um Comité de GCN, que pode desempenhar estas funções de acordo com Manoel S.S (2019, p.111).

Embora não esteja claro na referência anterior, entende-se que a criação de um Comité de GCN não retira qualquer responsabilidade à Administração de uma organização, mas permite que seja formalizada uma delegação de competências de determinadas funções.

Embora os desenvolvimentos das medidas de GCN possam não ser diretamente da responsabilidade da Administração, cabe à gestão de topo a sua revisão periódica, havendo obviamente acompanhamento regular das alterações que possam existir.

De acordo com a ISO 22301 (2019, p. 9.3.2) a revisão de qualquer Administração em funções, deve ter em consideração os seguintes aspetos:

- Ponto de situação sobre a medidas a serem tomadas após revisões anteriores;
- Alterações de problemas internos ou externos que possam ser relevantes para o *Business Continuity Management System* (BCMS);
- Informação sobre o desempenho do BCMS, incluindo-se:
    - Não conformidades e medidas corretivas;
    - Monitorização e quantificação dos resultados das avaliações;
    - Resultados das auditorias
- Feedback das partes interessadas;
- Necessidade de alterações ao BCMS incluindo a política e os objetivos;
- Procedimentos e recursos que possam ser utilizados para melhorar o desempenho e a eficácia do BCMS;
- Informação sobre as BIA's e análises de risco;
- Resultados da avaliação da documentação sobre a continuidade de negócio;
- Riscos e problemas não canalizados corretamente em análises de risco anteriores;
- Lições retiradas e ações que surgem de eventuais falhas ou eventos que causam dirupções das atividades;
- Oportunidades de melhoria contínua.

2.6 Estratégias de um SGCN

Cabe a cada organização com base nos resultados das BIA's e de avaliação de risco, definir as estratégias adaptadas à sua realidade, que permitam obter soluções para o antes, durante e após um evento diruptivo.

De acordo com a ISO 22301:2019 (p. 8.3.2) a identificação das estratégias e soluções devem:

- *«meet the requirements to continue and recover prioritized activities within the identified time frames and agreed capacity»;*
- *«protect the organization's prioritized activities»;*
- *«reduce the likelihood of disruption»;*
- *«shorten the period of disruption»;*
- *«limit the impact of disruption on the organization's products and services»;*
- *«provide for the availability of adequate resources».*

Para que possam ser implementadas as soluções de continuidade de negócio, as organizações devem definir requisitos para os recursos necessários, que de acordo com a ISO 22301:2019 (p.8.3.4) entre outros, podem ser:

- Humanos;
- Informação;
- Infraestruturas, como edifícios, locais de trabalho ou outros;

- Equipamentos e consumíveis;
- Sistemas de Informação;
- Transportes e Logística;
- Financeiros;
- Fornecedores e outros parceiros.

2.7 Incorporar Políticas de Continuidade de Negócio na Organização

Incorporar políticas de continuidade de negócio numa empresa quando estas não fazem ainda parte da cultura organizacional pode ser desafiante. De acordo com a revisão da literatura efetuada é um passo fundamental para o sucesso das mesmas.

O *Business Continuity Institute* (BCI) na sua página Internet e à data da consulta realizada sobre «*how to embed business continuity into your organization*» apresenta cinco recomendações fundamentais para o sucesso de uma introdução de políticas de continuidade de negócio nas organizações e que são as seguintes:

- *Use a collaborative approach;*
- *Make sure top-management is involved;*
- *Engage your staff;*
- *Raise awareness in an innovative way;*
- *Invest in your team.*

De forma a que toda organização adote uma cultura de continuidade de negócio é importante que na introdução destas políticas corporativas todos os departamentos/equipas estejam de alguma forma envolvidos neste processo utilizando assim uma abordagem colaborativa.

Importa consciencializar toda a organização das vantagens da existência de políticas de continuidade de negócio.

Citando o BCI na sua página internet «[t]*his will help each team understand how they can benefit from business continuity and how collaborating with other teams can make them more resilient.*»

Na importância de envolver todas as áreas funcionais, importa destacar a importância da liderança e o envolvimento da gestão de topo de forma a que o processo de incorporação das medidas ocorra no sentido de cima para baixo, ou seja, partindo da estratégia definida para as áreas operacionais.

Envolver os colaboradores na elaboração e implementação de políticas de continuidade de negócio é outro aspeto importante para garantir o sucesso das mesmas. O BCI indica como recomendação neste sentido, «*build a team of influential individuals within the organization who understand the benefits of business continuity and building organizational resilience that can act as advocates*», de forma a que estes colaboradores possam influenciar de forma positiva o resto da organização a tornar-se mais resiliente.

A procura de formas criativas para aumentar a consciencialização sobre continuidade de negócio, pode determinar o sucesso da adoção destas políticas, contribuindo positivamente para a motivação dos colaboradores neste sentido. Entre outras possibilidades o BCI sugere *«webinars, posters, white papers, training opportunities»*.

Por último, relativamente a recomendações do BCI sobre incorporação das políticas de continuidade de negócio, surge o investimento nas equipas como sendo «*the best thing you can do if you wish to embed business continuity within your organization»*.

O investimento nas equipas pode surgir de diversas formas, entre as quais a partilha de informação como *white papers* ou *research reports* e principalmente, a aposta na formação, podendo esta ser terceirizada para organizações especialistas nestas matérias.

2.8 Âmbito dos SGCN

A definição do âmbito de um SGCN é uma informação fundamental. Deve ser documentada numa fase inicial na criação dos planos. Será no âmbito das políticas de continuidade de negócio que se define se a organização vai elaborar medidas apenas para eventos relacionados com tecnologias de informação (TI) por exemplo, ou se vai alargar a mais áreas e se existe a necessidade de mapear processos interfuncionais na organização. (Manoel S.S 2019, p.99).

A definição do âmbito passa em parte por definir quais serão os limites até onde vão as medidas de continuidade de negócio podendo assim ficar delimitada a abrangência dos planos.

Em princípio, um âmbito bem suportado e definido, não irá sofrer muitas alterações no futuro a não ser que os próprios objetivos estratégicos da organização ou regulamentação associada, alterem ao longo do tempo.

Como uma forma de apoio na definição do âmbito de um SGCN, Manoel S.S (2019, p.100) indica as seguintes questões que podem ajudar a apurar evidências sobre este tema:

- Qual é a missão e a visão da organização?
- Quais são os objetivos estratégicos?
- Quais são as principais responsabilidades legais e regulatórias?
- Onde se localiza a organização e qual é o seu perímetro físico?
- Quais são os ativos físicos, tecnológicos, processos e pessoas?
- Quais são as pessoas envolvidas?
- Quais os produtos/serviços vendidos pela organização?
- Qual o mercado físico e global onde está inserida a organização?
- Quem são os clientes?
- Quais os processos que devem estar mapeados?
- Quem são os fornecedores e quais os serviços ou produtos que vendem?

2.9 Continuidade de negócio na gestão de risco

A CMVM *et al* (2010 p.6) refere que "[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".

A continuidade de negócio tem um papel importante na gestão de risco global de uma organização, afetando transversalmente toda a empresa, cruzando com processos ou subprocessos críticos para a organização como um todo.

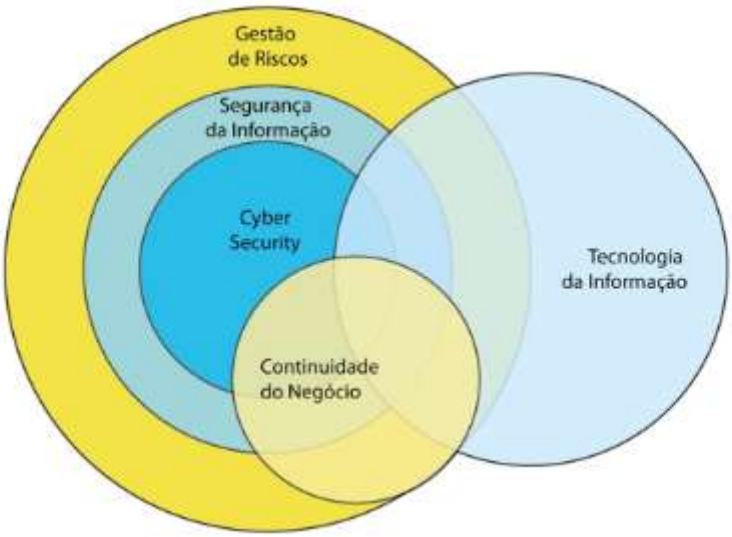

Figura 2.2 Posição da Continuidade de Negócio na Gestão de Risco

Fonte: Manoel S.S (2019 p.52)

3 PLANO DE CONTINUIDADE DE NEGÓCIO (PCN)

3.1 Definição

O *Disaster Recovery Institute International* (DRII) em 2018 no glossário para a resiliência, define um *Business Continuity Plan* (BCP) - designação internacional para PCN - como um conjunto de procedimentos e informações, devidamente documentados e desenvolvidos, que estão prontos para ser postos em execução a qualquer momento em caso de ocorrência de um evento disruptivo.

Estes procedimentos permitem à organização dar continuidade aos seus produtos ou serviços a um nível aceitável ao que é previamente definido.

Neste mesmo glossário publicado pelo DRII em 2018, um evento disruptivo é definido com um acontecimento que de alguma forma interrompe as operações ou processos da organização. Estes acontecimentos podem ser previsíveis ou antecipados como é o caso de tempestades ou crises políticas, ou podem-se tratar de eventos que não podem ser antecipados como um *Blackout,* ataque terrorista ou falha tecnológica.

Um PCN, definido pela CMVM *et al* (2010, p. 15/16) passa pelo seguinte:

> constitui um plano de ação detalhado que estabelece as medidas e os procedimentos necessários para a recuperação da atividade 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 atividade, incluindo o processo de retorno, com a maior brevidade possível, a níveis de qualidade de serviço normais.

De acordo com o *IT Gorvernance* (2019) a continuidade de negócio é uma disciplina que se foca primariamente em preservar a capacidade que uma organização tem em funcionar durante um evento disruptivo, assegurando que as suas funções mais críticas continuam, mesmo que com uma capacidade mais reduzida.

A KPMG (2006) indica que a disciplina de BCP ajuda as organizações na gestão de risco para os sistemas críticos, como o caso das redes partilhadas de informação e comunicação, contra eventos de causas naturais, eventos com intervenção humana ou mesmo motivos políticos, que de alguma forma ponham em causa a capacidade de continuar o negócio dentro da normalidade.

A KPMG (2016) define a sua abordagem a um BCP assente em sete pontos essenciais que cobrem todo o ciclo de vida da gestão de continuidade de negócio. São eles:

- Análise de impacto no negócio;
- Avaliação de ameaças e vulnerabilidades;
- Definição dos ativos críticos para o negócio;
- Definição da estratégia de continuidade de negócio;
- Preparação do PCN e Plano de Recuperação de Desastre (PRD);

- Testes e formações;
- Manutenção.

De acordo com Jorrigala (2018) um PCN é composto por:

- Gestão do PCN;
- BIA's;
- Planeamento das medidas para por em prática o PCN;
- Dependência do estado de prontidão do PCN;
- Testes, manutenção e auditoria ao PCN.

Uma componente de elevada importância num PCN é a existência de planos de comunicação que permitam que a informação chegue onde tem de chegar em momentos de maior disrupção. De acordo com a CMVM *et al.* (2010, p 8) «[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».

As organizações devem documentar os seus PCN e os diversos procedimentos que os compõem. De acordo com a ISO 22301:2019 (p.8.4.1) estes procedimentos devem ser:

- específicos quanto às medidas a serem colocadas em prática durante um evento disruptivo;
- flexíveis de forma a responderem a alterações internas ou externas da dirupção;
- focados no impacto dos incidentes que levaram à disrupção;
- eficazes em minimizar os impactos durante a implementação de soluções apropriadas;
- elaborados de forma a definir funções e responsabilidades para as diferentes tarefas.

3.2 Objetivos

De acordo com Bronack (2012), um bom PCN deve conter nos seus objetivos:

- Proteção dos colaboradores;
- Recuperação de processos ou funções críticas para o negócio de forma a minimizar o impacto do desastre;
- Recuperação de infraestruturas e sistemas de suporte às funções consideradas críticas;
- Prevenção e mitigação dos efeitos de um desastre possível de ocorrer a qualquer momento;
- Proteção dos ativos da organização;
- Minimização dos impactos negativos do ponto de vista legal.

As organizações devem documentar os objetivos do PCN e segundo a ISO 22301:2019 (p.6.2.1) estes objetivos devem ser:

- Consistentes com as políticas de continuidade de negócio;
- Mensuráveis;
- Monitorizados;
- Comunicados;
- Atualizados de forma apropriada.

3.3 Responsabilidade sobre os PCN

Uma das características dos PCN referida por vários autores é a definição de responsabilidades nas diversas medidas a serem colocadas em prática com a ativação do plano.

Igualmente importante e que cada organização deve ter um papel bem definido é a responsabilidade sobre o próprio PCN em si mesmo.

Num questionário a tomadores de decisões de empresas canadianas publicado pela KPMG (2006) é referido que o desenvolvimento de um PCN deve envolver não só os principais fornecedores de SI, mas também todas as áreas que utilizam esses mesmos sistemas e a própria administração. A cultura de continuidade deve ser transversal a toda a organização, com os papeis bem definidos com processos de responsabilidades e reportes devidamente implementados. Uma das principais dificuldades será a de manter a gestão consciente da importância de considerar os PCN no planeamento estratégico, operacional e orçamental das atividades.

Quanto à responsabilidade pelo PCN, a CMVM *et al* (2010 p.7) refere que «o órgão de administração deve considerar a gestão da continuidade de negócio como constituindo parte integrante da gestão de risco, [..] sendo os responsáveis máximos pela implementação e desenvolvimento da política de gestão da continuidade de negócio." Ainda sobre este assunto os autores referem na mesma página que:

> [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.

Desta forma define-se que a GCN, sendo uma função partilhada por vários membros da empresa, em diversas funções, ou havendo um departamento a trabalhar em específico para este fim, a administração terá sempre a responsabilidade sobre o que ficar definido, o que traz uma elevada importância e exigência ao desenvolvimento destes planos. A questão de haver recursos exclusivos para a continuidade de negócio ou não é uma questão que irá sempre depender da dimensão e complexidade da organização em causa.

Dentro das responsabilidades sobre os PCN, a CMVM *et al.* (2010, p7) refere que cabe ao órgão de administração:

> 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 da gestão da continuidade de negócio, nomeadamente através da afetação, a esta política, de recursos humanos e financeiros em quantidade e qualidade suficientes para assegurar uma implementação abrangente e robusta.

3.4 Análise de Impacto no Negócio

As BIA's de acordo com o vocabulário da norma internacional ISO 22300 que incide sobre segurança e resiliência, são definidas como a análise das atividades e processos, bem como, qual o efeito que eventos diruptivos nestes podem ter no negócio.

De uma forma mais simples, mas cujo conceito se aproxima ao apresentado anteriormente, o DRII (2018) no seu glossário define as BIA's como *«[a] method of identifying the effects of failing to perform a function or requirement»*.

Reforçando esta ideia, a KPMG (2016) define as BIA's como o processo que identifica e ordena por importância, as atividades e os ativos críticos para o negócio, bem como, o tempo máximo aceitável que estes podem estar sem funcionar e quando podem ser reativados.

De acordo com o DRII (2018) no guia das práticas profissionais os objetivos das BIA's passam por:

- Identificar e ordenar por prioridade as funções e processos de forma a definir quais terão maior impacto na organização em caso de falha;
- Avaliar quais os recursos necessários para suportar os processos de análise de impacto no negócio;
- Analisar os resultados obtidos e identificar eventuais diferenças entre os requisitos da organização e a sua capacidade de cumprir com esses requisitos.

De acordo com a CMVM *et al* (2010) as BIA's como base do processo de GCN consistem 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 atividade, na reputação, na situação financeira e/ou nas contrapartes da instituição;
- Identificar as infraestruturas que dão suporte a essas funções de negócio críticas, em particular as de cariz tecnológico;
- Identificar a existência de dependências internas e externas relativamente a essas funções de negócio.

No documento acima referido, são ainda identificadas as várias fases que devem fazer parte das BIA's, relevando-se as seguintes:

- Identificação dos riscos suscetíveis de gerar uma interrupção da atividade e que possam originar um impacto material para a instituição;
- Identificação de cenários de interrupção plausíveis, incluindo estimativas das respetivas probabilidades de ocorrência e da duração provável dos seus efeitos;
- 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;
- Impacto financeiro, legal e reputacional da interrupção de funções de negócio críticas sobre a instituição, considerando períodos de tempo diversos.

No seguimento desta última referência importa ainda evidenciar um detalhe sobre a importância da resposta a consequências de determinados cenários ou eventos e não sobre a procura da origem destes. «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» (CMVM *et al,* 2010, p.9). As origens dos diversos cenários serão importantes apenas na justificação da plausibilidade destes. É importante ainda evidenciar:

> [e]m particular, para além de ser necessário que a seleção das funções de negócio críticas traduza, efetivamente, as prioridades, os procedimentos a sistematizar e os recursos (humanos e materiais) a mobilizar, aquela deve também refletir as condições em que o negócio é normalmente desenvolvido. Além disso, a política de continuidade de negócio deve ser objeto de ajustamento contínuo ao desenvolvimento do negócio. (CMVM *et al,* 2010, p 8).

Neste sentido, se considerarmos que o processo que define a seleção das funções de negócio críticas, as BIA's, podemos deduzir com base neste documento, que uma das suas bases é a definição daquilo que é o normal funcionamento das atividades da empresa. A partir daqui estaremos então em condições de definir aquilo que serão as situações de disrupção.

A ISO 22301:2019 (p. 8.2.2) vem definir os procedimentos das BIA'S de uma forma semelhante aos já apresentados, mas que permite complementar as ideias apresentadas da seguinte forma:

- *define the impact types and criteria relevant to the organization's context;*
- *identify the activities that support the provision of products and services;*
- *use the impact types and criteria for assessing the impacts over time resulting from the disruption of these activities;*
- *identify the time frame within which the impacts of not resuming activities would become unacceptable to the organization (maximum tolerable period of disruption "MTPD")*
- *set prioritized time frames within the time identified in "MTPD" for resuming disrupted activities at a specified minimum acceptable capacity (recovery time objective "RTO")*
- *use this analysis to identify prioritized activities;*

- *determine which resources are needed to support prioritized activities;*
- *determine the dependencies, including partners and suppliers, and interdependencies of prioritized activities.*

Para que as BIA's possam ser efetivamente de utilidade é importante que sejam respondidas, algumas questões que Bronack (2012) define como:

- As BIA's desenvolvidas estão documentadas e alinhadas com os critérios definidos?
- Está estabelecida uma metodologia para desenvolver as BIA's e documentar os resultados?
- As BIA's finais foram aprovadas pela Administração?
- As estratégias da recuperação estão alinhadas com os resultados das BIA's?
- Existe documentação para as premissas utilizadas, bem como, um racional de classificação por importância do impacto?
- Os *Recovery Time Objetives* (RTO) e *Recovery Point Objectives* (RPO)estão identificados?

De acordo com o DRII (2018), o RTO é o tempo definido como objetivo para a restauração e recuperação das funcionalidades ou recursos, com base num tempo máximo aceitável que estes podem estar em baixo e o seu nível de desempenho em caso de um evento disruptivo.

Todavia, o RPO é definido como o ponto para o qual a informação utilizada por uma atividade deve ser restabelecida, ou de uma forma mais simples, o máximo de informação que pode ser perdida.

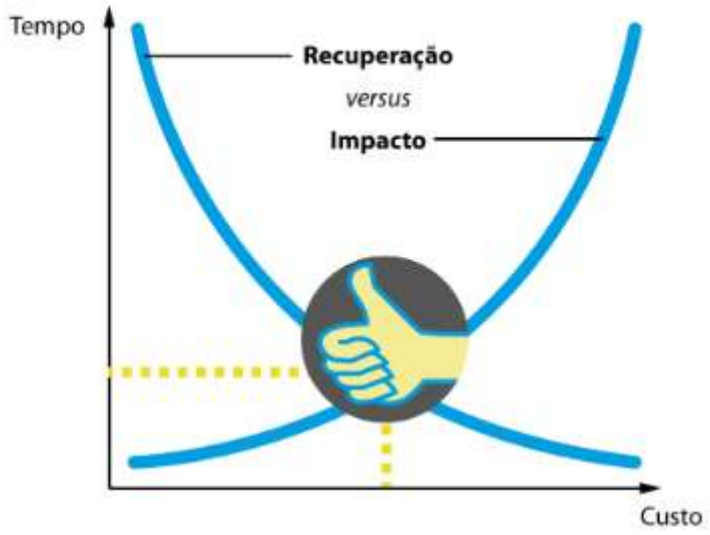

Figura 3.1 Relação Custo x Tempo

Fonte Manoel S.S. (2019 p.202)

Na Figura 3.1 é possível observar um gráfico demonstrativo da relação entre o custo e o tempo de recuperação e impacto numa organização. A organizações dentro das suas possibilidades, devem encontrar um ponto de equilibro razoável para a realidade em que se inserem.

Quanto menor for o tempo de recuperação (RTO) maior será o custo, ou seja, quanto menor o valor investido também maior será o impacto na organização. (Manoel S.S, 2019, p201).

Cabe aos profissionais de GCN de acordo com o DRII (2018):

- Identificar os critérios qualitativos e quantitativos a serem usados na avaliação do impacto na organização, após um evento;
- Obter consenso com as chefias diretas sobre a metodologia da análise de impacto de negócio e os critérios utilizados para a definir, bem como, os seus processos;
- Planear e coordenar a recolha de informação e análise a ser feita;
- Estabelecer os critérios e a metodologia a serem utilizados na execução das BIA's;
- Analisar a informação recolhida e aplicar os critérios previamente definidos para chegar ao RTO e RPO;
- Preparar e apresentar os resultados das BIA's e obter aprovação do RTO e RPO.

Conforme referido anteriormente as BIA's são um dos pontos mais essenciais na formação das políticas de continuidade de negócio, mas podem ter mais utilidades além de servir apenas para a definição dos planos. Manoel S.S (2019, p.42) refere-se às análises de impacto no negócio como «uma ferramenta para a tomada de decisão».

Por vezes a gestão de topo pode ter dificuldades em identificar onde deve investir na organização para conseguir um maior retorno e as BIA's fazem exatamente esta tarefa, «informando quais os processos que são mais críticos para a organização, portanto informa quais são os processos de negócio que angariam mais dinheiro e principalmente quais são os ativos que suportam esses processos e precisam ser protegidos» (Manoel S.S, 2019, p.42).

A execução das BIA's permite a uma organização, de acordo com Manoel S.S (2019, p.174), identificar medidas que:

- Limitem o impacto negativo de uma interrupção nos processos de negócio;
- Diminuam o período de interrupção;
- Diminuam a probabilidade de haver interrupção.

3.5 Fases de um PCN

Um PCN tem diversas fases desde ser acionado, até ao momento em que já não está em prática (retorno à normalidade). O SANS *Institute* publicou em 2006 e dividiu os PCN em fases. São as seguintes:

- Resposta ao incidente ou fase de ativação;
- Resolução do problema;
- Retorno à normalidade das operações ou fase de recuperação.

Na eventualidade da ocorrência de eventos que ponham em risco o normal funcionamento das operações, o PCN pode ser acionado. O tipo de eventos disruptivos que levam à ativação do PCN, segundo o SANS *Institute* podem ser:

- Ameaças à segurança dos colaboradores;
- Ameaças à segurança das infraestruturas;
- Ameaças ao ambiente onde a organização está inserida;
- Ameaças a infraestruturas críticas e essenciais para as operações (energia, abastecimento de água, comunicações);
- Ameaças às operações a nível de processos, fornecedores ou parcerias críticas.

O PCN apenas é dado como terminado quando as infraestruturas, serviços ou pessoal afetados voltam a operar dentro da normalidade, estando concluída assim a recuperação.

3.6 Estratégia de Recuperação de Negócio

De acordo com a CMVM *et al* (2010, p.10) a estratégia de recuperação de negócio que deve ter por base as BIA's, deve traduzir-se na definição de:

- Objetivos de recuperação, os quais constituem as metas predefinidas quanto à recuperação de funções de negócio críticas, de acordo com um nível de serviço específico (RPO) dentro de um determinado período de tempo (RTO), após uma interrupção grave e não planeada da atividade;
- Prioridades na recuperação das funções de negócio críticas, de acordo com o impacto potencial no desenvolvimento do negócio, na rentabilidade ou na reputação;
- Prioridades na recuperação das infraestruturas tecnológicas que dão suporte às funções de negócio críticas.

3.7 Infraestruturas Alternativas

A CMVM *et al* (2010, p.12) define em relação às infraestruturas físicas alternativas, que estas podem ter diversos graus de preparação, incluindo:

- 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 no dia-a-dia, estão disponíveis para a execução das funções de negócio críticas em caso de contingência, embora requerendo a sua ativação prévia ("*cold sites*");
- Infraestruturas 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.

Embora não seja referido no texto original o último ponto enunciado anteriormente é normalmente denominado por *warm site.*

Quanto a infraestruturas informáticas alternativas, a CMVM refere que a periodicidade da salvaguarda de dados deve ser feita de acordo com os tempos de recuperação estabelecidos inicialmente. Citando a CMVM novamente «[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 atividade contínua da instituição» (CMVM *et al,* 2010, p.13).

A dimensão das empresas pode por vezes condicionar a possibilidade da existência deste tipo de infraestruturas alternativas, sendo muitas vezes a terciarização deste tipo de serviços uma opção que se compreende e aceita.

3.8 Coordenação com Terceiros

Quanto à coordenação e gestão da dependência de terceiros em caso de crise a CMVM *et al* (2010, p.13) refere que 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».

Neste sentido, sendo este último documento direcionado a instituições bancárias e a seguradoras, será espectável que enquanto fornecedor destas entidades, especialmente se existir uma elevada dependência da organização em determinados fornecimentos, seja exigida alguma prova da existência de estratégias de recuperação.

No desenvolvimento da presente investigação, numa das entrevistas possíveis com um responsável do departamento de risco operacional de uma organização do setor bancário a atuar em Portugal, foi possível abordarmos livremente este assunto. Consequentemente, foi referido que por vezes podem ser adicionadas cláusulas de continuidade de negócio em determinados tipos de contratos.

3.9 Comunicação

É um dos pontos chave de um robusto PCN. A comunicação nas suas diversas formas deve estar contemplada sobre a viabilidade por onde se irá transmitir a informação, bem como, onde esta informação irá chegar.

A CMVM *et al* (2010, p14) divide a comunicação em três tipos:

- Comunicação interna - dentro da própria empresa, entre colaboradores a todos os níveis;
- Comunicação externa - com outras instituições com autoridades de supervisão, com clientes, com a imprensa, ou com o público em geral;
- Comunicação intermédia - com as famílias dos colaboradores quando estiver em causa a integridade física dos mesmos ou caso estes não consigam estabelecer comunicações.

Como nos mais diversos aspetos condizentes com a continuidade de negócio, também em relação à comunicação, as entidades devem documentar os diversos procedimentos existentes, que de acordo com a ISO 22301:2019 (p.8.4.3.1) podem ser:

- Comunicação interna e externa para as diversas partes interessadas questionando o quê, quando, com quem e como comunicar;
- Receber, documentar e dar resposta a comunicações das mais diversas entidades interessadas;
- Assegurar a disponibilidade de meios de comunicação durante um evento disruptivo;
- Facilitação de comunicação estruturada com entidades de resposta a emergências;
- Detalhar a comunicação com a imprensa após um incidente, incluindo a estratégia a seguir neste sentido;
- Documentar e gravar os detalhes da disrupção, as medidas e as decisões tomadas;
- Alertar partes interessadas que possam potencialmente ser afetadas por eventos disruptivos eminentes.

3.10 Manutenção, Melhoria Contínua e Periodicidade de Testes a PCN

Perante a investigação realizada, a manutenção de um PCN é, entre outros, feita através de testes, simulações e formações. Deve ser um dos pontos chave para o sucesso na sua implementação, pois será através da boa aceitação que se abre caminho à melhoria contínua.

Um processo de melhoria contínua deve ocorrer de forma natural com os resultados de análises feitas aos planos, relatórios de auditorias ou ainda, através de um relatório de avaliação feito pela gestão. Além destes exemplos, os processos de melhoria podem derivar de alterações na própria organização em termos de processos, pessoal ou recursos. Alguns exemplos dados por Manoel (2019, p.327) de alterações com impacto, passam por:

- Introdução de novos produtos e consequentemente novos procedimentos;
- Alteração na forma como um fornecedor aceita os pedidos;
- Um novo pacote que envolva reformas antecipadas e que leve à saída de membros mais seniores da organização.
- Alteração na formação das equipas de TI em que os seus membros tinham papéis fundamentais nos planos existentes;
- Alteração da forma como é feito o fornecimento da rede que suporta os sistemas críticos da organização, deixando por exemplo de funcionar por cabo e passando a ser por redes sem fios (*wi-fi*).

Relativamente aos testes, a CMVM *et al* (2010, p.17) refere que estes podem ser diversos quanto à abrangência, sendo expectável que as organizações complementem testes mais específicos com outros mais completos e que incidam sobre diversos componentes do PCN.

Sendo as próprias organizações as responsáveis pela elaboração dos testes ou simulações, a CMVM *et al* (2010 p.18) define quanto à periodicidade destes que é expectável «que as instituições de maior dimensão e complexidade realizem testes de maior amplitude com periodicidade, no mínimo, anualmente», deixando, no entanto, a recomendação de que estes testes sejam feitos com maior frequência.

Além da periodicidade dos testes, importa ainda referir que o PCN seja na sua globalidade revisto e eventualmente atualizado em conformidade com as necessidades identificadas, definindo a CMVM *et al* (2010, p.18) também, o mínimo de um ano, para esta revisão.

> [o] PCN deve ainda ser sujeito a uma revisão por parte dos auditores internos da instituição ou através de mecanismos equivalentes que se adequem à dimensão, natureza e complexidade da sua atividade, sem prejuízo de auditoria externa, caso a instituição a entenda importante nesta matéria. 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.

As organizações devem procurar de uma forma contínua a melhoria das suas políticas de continuidade de negócio e adaptá-las à evolução da própria organização. De acordo com a ISO 22301:2019 (p. 10.2) «*[t]he organization shall continually improve the suitability, adequacy and effectiveness of the BCMS, based on qualitative and quantitative measures*». A norma refere ainda que, as organizações devem considerar a possibilidade de existirem oportunidades de melhoria através da análise dos resultados das avaliações feitas e revisões propostas pela administração.

Quanto à caracterização dos exercícios ou testes feitos aos PCN, a ISO 22301:2019 (p. 8.5) indica que estes devem:

- Ser consistentes com os objetivos de continuidade de negócio;
- Ser baseados em cenários apropriados bem planeados e com objetivos claros;
- Desenvolver trabalho de equipa, competências, confiança e conhecimento para os envolvidos;
- À medida que os exercícios ou testes são feitos em conjunto, validam-se as estratégias e as soluções de continuidade de negócio;
- Produzir relatórios com os resultados, recomendações e ações a tomar para implementar melhorias;
- Ser revistos no âmbito da melhoria contínua;
- Ser feitos em intervalos de tempo planeados e adicionalmente, quando existam grande alterações no contexto da organização.

3.11 Considerações sobre um bom PCN

Em linha com as ideias referidas anteriormente, as várias características referidas devem estar documentadas no PCN. Este deve estar disponível para todas a pessoas envolvidas.

É importante que o acesso ao PCN seja do conhecimento geral dos envolvidos e deve ser pensada uma forma de acesso na eventualidade das vias habituais não estarem disponíveis, por exemplo, através de cópias de segurança noutras localizações. Em resumo, a CMVM *et al* (2010, p. 16 e 17) define que no mínimo, um PCN para funcionar de forma eficaz e eficiente, deve conter pelo menos os seguintes aspetos:

- Identificação clara da estrutura de coordenação das questões relacionadas com a GCN, incluindo os respetivos papéis, responsabilidades e autoridades para atuação 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 respetivos níveis de recuperação e tempos de recuperação;
- Identificação das infraestruturas, 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 ativação do PCN, que tenham em conta, pelo menos, a potencial gravidade do impacto na atividade da instituição e os objetivos de recuperação previamente definidos;
- Procedimentos e critérios específicos que cubram a possibilidade de ativação do centro de processamento alternativo, incluindo-se procedimentos para deslocação do pessoal;
- Identificação do conjunto de colaboradores a convocar para operar em situação de contingência, incluindo-se os respetivos contactos fora de horas;
- Procedimentos para a convocatória dos colaboradores designados para operar em situação de contingência, incluindo-se métodos que permitam estabelecer contacto imediato com os substitutos, no caso de os primeiros estarem inacessíveis;
- Procedimentos e outra informação que permitam restabelecer as funções de negócio críticas e/ou de operação em contingência, incluindo-se, as que sejam desempenhadas por entidades subcontratadas;
- Procedimentos e outra informação que permitam ativar as infraestruturas 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 permita recuperar ficheiros e documentação crítica;
- Plano de comunicação com os colaboradores da organização e outras partes interessadas;
- Procedimentos e outra informação que permitam o retorno à atividade normal;
- Um PCN deve conter informação sobre a manutenção e a periodicidade da realização de testes ou simulações.

Importa esclarecer que o documento referido está especificamente direcionado ao setor financeiro, em concreto o setor bancário, segurador ou outro supervisionado pelas entidades que criaram o documento. No entanto, muitos dos aspetos referidos são abstratos o suficiente para que possam, ao critério de quem elabora os PCN, ser transpostos para outro tipo de organizações com as devidas adaptações.

Como referido anteriormente uma GCN envolve a elaboração de PCN. É recomendado que a elaboração seja feita tendo em conta as características especificas da organização onde se vai aplicar. Quaisquer recomendações por mais abstratas que sejam, devem ser adaptadas a uma realidade específica.

3.12 Diferenças para o Plano de Recuperação de Desastre (PRD)

Para diferenciar um PCN de um PRD, importa definir que, segundo o glossário para a resiliência do DRII (2018), este último trata-se de um plano que visa a recuperação de um ou mais sistemas, num local alternativo como resposta a um evento que tenha causado a interrupção das operações.

O BCI em 2017 e em parceria com o *Disaster Recovery Journal* (DRJ) referiu no glossário dos termos de PCN, a definição de *Disaster Recovery* (DR) como sendo o processo, políticas e procedimentos relacionados com a preparação para recuperação e continuidade das infraestruturas tecnológicas, sistemas e aplicações que são vitais para a organização após a ocorrência de um desastre.

Como nota é ainda referido que a DR está focada na informação ou sistemas tecnológicos que são a base para o funcionamento da organização, enquanto a Continuidade de Negócio implica um planeamento, que visa manter todos os aspetos essenciais do negócio em funcionamento durante a ocorrência de um desastre.

De acordo com o BCI, a recuperação de um desastre, é um subconjunto da Continuidade de Negócio.

É importante referir ainda que no glossário publicado pelo BCI & DRJ em 2017, um PRD é definido como um documento aprovado pela gestão que define os recursos, ações, tarefas e informação necessários para gerir a recuperação da tecnologia. Por norma, refere-se à recuperação de elementos tecnológicos essenciais afetados por um evento disruptivo.

De acordo com o *IT Gorvernance* (março, 2019) a recuperação de desastre enquanto disciplina diferenciada da CN, foca-se na recuperação para as capacidades plenas dos recursos relacionados com SI, após um evento disruptivo.

Desta forma a recuperação de desastre deve abranger um vasto leque de possíveis eventos disruptivos e para cada um deles uma solução para a recuperação total dos SI.

A distinção para a Continuidade de Negócio está, em que esta, não visa apenas a recuperação das funcionalidades, mas sim garantias de que no caso de um evento disruptivo as funcionalidades previamente definidas como cruciais, continuam a operar mesmo que a um nível mínimo de capacidade.

4 EVENTOS DISRUPTIVOS E OS SEUS IMPACTOS

4.1 Principais Eventos Disruptivos

Anualmente a organização BCI publica um relatório com a análise dos principais eventos causadores de disrupções nos últimos 12 meses, bem como, uma previsão dos próximos 12 meses. É de evidenciar que no relatório publicado em 2020, a elevada importância dos incidentes relacionados com doenças ocupacionais, são a principal causa de disrupção nas organizações.

Embora o relatório referido destaque eventos relacionados com doenças ocupacionais como os mais causadores de disrupções nos últimos 12 meses que antecedem o relatório, os ciberataques constam como os eventos que mais preocupam para os 12 meses futuros, baseados em inquéritos realizados. Esta é uma informação que não considera os impactos da pandemia COVID-19, uma vez que os inquéritos foram realizados antes da propagação da pandemia.

Figura 4.1 Análise de Riscos e Ameaças nos últimos 12 meses, próximos 12 meses e consequências das disrupções, tendo por base inquéritos realizados em 2020

Fonte BCI Horizon Scan Report 2020 *(p.7)*

O ano de 2019 é o primeiro desde 2014 em que os ciberataques não são a principal causa de disrupção nas organizações, tendo dado lugar às doenças ocupacionais que não incluem as pandemias como o caso do COVID-19 de grande impacto durante o final 2019 e a acontecer ao longo de 2020.

[c]ountry legislation often requires all health incidents to be recorded and monitored which could influence an organization's ability to more accurately track and monitor this kind of incident. In contrast, smaller IT or telecom outages may not be so diligently recorded. (BCI Scan Report, 2020, p.11)

Com o surgimento da pandemia COVID-19 em diversos continentes e com maior intensidade no início de 2020, tendo os primeiros casos sido relatados no final de 2019 na China, é muito elevada a probabilidade de os eventos disruptivos relacionados com a saúde se manterem a principal causa de disrupção nos próximos tempos.

Importa por isso que as organizações dirijam as suas estratégias de CN neste sentido, não esquecendo todas as outras possíveis formas de disrupção, alterando desta forma os trabalhos de auditoria a realizar sobre estes temas, cobrindo de forma mais completa todas estas novas preocupações emergentes.

	Ranking	Frequency
1	Health incident (occupational disease, reportable occupational disease, stress/mental health, increased sickness absence)	7.5
2	IT and telecom outage	6.4
3	Safety incident (personal injury, fatality, asset damage, dangerous occurrence, reportable incident)	6.7
4	Lack of talent/key skills	5.6
5	Cyber-attack & data breach	6.1
6	Non-occupational disease	5.9
7	Product safety recall	5.2
8	Extreme weather events (e.g. floods, storms, freeze, etc.)	5.1
9	Interruption to utility supply	5.3
10	Exchange rate volatility	5.1
11	Natural resources shortage	4.9
12	Lone attacker/active shooter incident	4.5
13	Political violence/civil unrest	4.7
14	Introduction of new technology (IoT, AI, Big data)	4.6
15	Regulatory changes	4.3
16	Critical infrastructure failure	4.0
17	Higher cost of borrowing	4.6
18	Enforcement by regulator	3.9
19	Natural disasters (earthquakes, tsunamis, etc.)	4.0
20	Supply chain disruption	4.3
21	Energy price shock	4.3
22	Political change	3.9

Figura 4.2 Lista de riscos causadores de disrupção nos últimos 12 meses, base 2020

Fonte: *BCI Horizon Scan Report* 2020 (p.14)

Os ataques informáticos estão no topo das atenções da maior parte dos profissionais, em grande parte porque estes ocorrem diariamente e obrigam regularmente as empresas a tomar ações preventivas e corretivas. No entanto este tipo de ataques na sua maioria não tem um impacto tão severo como um desastre natural ou uma pandemia, que ocorrem com menos frequência.

> *There are cyber-attacks all the time, but currently not so severe that our core area of responsibility is targeted and affected. "Solutions Manager, Technology, Netherlands"*(BCI Horizon Scan Report, 2020, p.12)

As organizações não podem deixar de estar preparadas para os vários casos e devem-se prevenir adequadamente para cada eventualidade.

Ranking		Likelihood
1	Cyber-attack & data breach	3.1
2	IT and telecom outage	3.0
3	Extreme weather events (e.g. floods, storms, freeze, etc.)	2.9
4	Critical infrastructure failure	2.3
5	Lack of talent/key skills	2.6
6	Regulatory changes	2.6
7	Natural disasters (earthquakes, tsunamis, etc.)	2.0
8	Interruption to utility supply	2.6
9	Introduction of new technology (IoT, AI, Big data)	2.6
10	Political change	2.4
11	Supply chain disruption	2.2
12	Safety incident (personal injury, fatality, asset damage, dangerous occurrence, reportable incident)	2.5
13	Lone attacker/active shooter incident	1.8
14	Enforcement by regulator	2.1
15	Health incident (occupational disease, reportable occupational disease, stress/mental health, increased sickness absence)	2.4
16	Political violence/civil unrest	2.1
17	Exchange rate volatility	2.1
18	Higher cost of borrowing	1.9
19	Energy price shock	1.9
20	Natural resources shortage	1.7
21	Non-occupational disease	1.8
22	Product safety recall	1.5

Figura 4.3 Lista de riscos causadores de disrupção nos próximos 12 meses (previsão), base 2020

Fonte: *BCI Horizon Scan Report 2020 (p.20)*

> *Non-occupational disease is second from bottom of the table. This year's Horizon Scan survey was carried out before the outbreak of Coronavirus at the end of 2019, showing how quickly the landscape can change.* (*BCI Horizon Scan Report, 2020, p19*).

No relatório acima referido, ressalva-se a diferença entre aquilo que foram os resultados dos questionários e apontada como principal preocupação futura e o que realmente se passou nos meses seguintes.

4.2 Consequências de Eventos Disruptivos

Os eventos causadores de disrupção podem ter impactos muito diferentes dependendo da capacidade que as organizações têm de mitigar as consequências com um adequado planeamento neste sentido ou até mesmo absorver por completo estas consequências. Por outro lado, há o caso de organizações que não estão de todo preparadas e por isso alteram por completo a sua estratégia, negócio, marca, ou no limite acabam por fechar.

Em 1988 no que é considerado por muitos o primeiro ataque informático em grande escala, de acordo com o site do *Federal Bureau of Investigation* (FBI) publicado em 2018, foi desenvolvido o primeiro *worm,* que é um tipo de software malicioso de propagação rápida que se replica a si mesmo, propagando-se por outros dispositivos.

Este software acabou por ser libertado via Internet, acabando por infetar em apenas 24 horas, segundo estimativas, cerca de 6.000 dos 60.000 equipamentos que na ocasião se encontravam ligados à Internet.

Este foi um evento histórico sem precedentes e do qual terão sido retiradas importantes lições, muito úteis para a atualidade.

Vivemos numa época tecnológica em constante evolução. No entanto, nem em todos os casos são os eventos tecnológicos que estão a causar maior impacto nas organizações.

De acordo com o *BCI Horizon Report 2020* conforme podemos verificar na Figura 4.2, são as alterações regulatórias que causam maior impacto financeiro nas organizações, aparecendo os ataques informáticos em apenas quinto lugar, segundo a referida lista.

	Disruption	Avg/disruption (€000)
1	Regulatory changes	1982.50
2	Safety incident (personal injury, fatality, asset damage, dangerous occurrence, reportable incident)	1525.00
3	Natural disasters (earthquakes, tsunamis, etc.)	1067.86
4	Extreme weather events (e.g. floods, storms, freeze, etc.)	1003.00
5	Cyber attack & data breach	745.00
6	Interruption to utility supply	625.00
7	Political violence/civil unrest	587.50
8	Interruption to utility supply	236.84
9	IT and telecom outage	189.23
10	Critical infrastructure failure	155.00

Figura 4.4 Custo médio por tipo de evento disruptivo

Fonte: *BCI Horizon Scan Report 2020 (p.28)*

5 CONTINUIDADE DE NEGÓCIO COMO EVENTO SEGURÁVEL

5.1 Cobertura de Interrupção de Atividade

Um aspeto adicional importante para as organizações que procuram as melhores formas de reduzir o impacto de interrupções no negócio pode ser a contratualização de seguros que visem cobrir potenciais perdas relacionadas com eventos disruptivos.

De acordo com o *Insurance Information Institute* (III), uma organização americana cujo principal objetivo é fornecer informação sobre seguros sem fazer qualquer tipo de comercialização dos mesmos, *«[b]usiness interruption coverage also known as business income coverage, can help with operating expenses during the period of restoration*».

A mesma fonte refere ainda sobre os tipos de cobertura existentes como sendo:

- Rendimentos líquidos com base em informação financeira histórica;
- Hipotecas, rendas e *leasings*;
- Impostos;
- Processamento salarial de empregados.

O III quanto a situações para as quais não existe por norma cobertura no *Business Interruption Insurance* indica as seguintes:

- Itens danificados como resultado de um evento segurado (exemplo: vidro);
- Danos causados por inundações ou terramotos que são cobertos por apólices diferentes;
- Rendimentos não documentados na informação financeira;
- Danos em infraestruturas;
- Pandemias, vírus ou outras doenças infeciosas (exemplo: COVID-19).

Os custos relacionados com a contratualização deste tipo de seguros irão depender de uma detalhada análise de risco que deve considerar, o tipo de negócio, número de empregados, avaliação de valores cobertos e o histórico da organização com a seguradora. Complementarmente, também a localização pode ser um fator diferenciador dos preços praticados, pois determinadas posições geográficas podem proporcionar maior exposição a determinados riscos que eventualmente causam interrupção na atividade (III, 2020).

No panorama nacional, diversas seguradoras apresentam soluções comerciais que incluem cobertura de perdas relacionadas com a interrupção da atividade, sendo uma forma de tornar mais robusta a cobertura destes tipos de riscos.

5.2 Seguradora Tranquilidade "Outros Seguros"

A seguradora Tranquilidade apresenta ao momento da consulta na sua página Internet e na secção "Outros Seguros" uma solução em que:

> [a]ssegura os prejuízos sofridos pela empresa resultantes da interrupção ou redução da sua atividade, em consequência de um sinistro de danos materiais que esteja garantido por um seguro de perdas diretas, também subscrito na Tranquilidade. Por exemplo, em caso de um sinistro coberto por uma apólice de multirrisco estabelecimento, o seguro de perdas de exploração garante eventuais prejuízos decorrentes da interrupção ou paralisação da atividade da empresa. A contabilização dos prejuízos provocados pela interrupção da atividade pode revestir diversas formas: lucro líquido, lucro bruto ou encargos permanentes da empresa

5.3 Seguradora Fidelidade "Multirriscos Negócios"

A Fidelidade, em alternativa, apresenta na sua solução "Multirriscos Negócios" entre as várias coberturas possíveis, desde incêndios, inundações, tempestades, entre outras, uma cobertura para a interrupção da atividade na organização.

Nas condições gerais disponibilizadas online a seguradora indica estar seguro

> [o] pagamento, até ao limite do valor fixado nas Condições Particulares, da indemnização diária contratada, durante a interrupção total da atividade, em consequência direta da verificação de um sinistro indemnizável ao abrigo das seguintes coberturas, quando contratadas.

As coberturas referidas são as seguintes:

- Incêndio, Ação Mecânica de Queda de Raio e Explosão;
- Tempestades;
- Inundações e danos por Água;
- Aluimento de Terras e fenómenos sísmicos;
- Atos de Vandalismo;
- Greves, Tumultos e Alterações da Ordem Pública.

Além das coberturas referidas, existe a possibilidade por exemplo de segurar os custos de reabertura da atividade relacionados com publicidade. Importa ter em consideração que todas estas condições são limitadas quanto ao tempo durante e até ao qual, existe a real cobertura.

5.4 Seguradora AIG "*CyberEdge*"

A seguradora AIG apresenta através da sua oferta "*CyberEdge*" à data da consulta na sua página Internet, uma solução concebida em específico para a cobertura de "riscos cibernéticos não cobertos por seguros de responsabilidade civil convencionais."

Este produto cobre riscos como a perda ou fuga de informação e que são muitas vezes causadores de pesadas multas.

O seguro cobre eventuais perdas financeiras relacionadas com a apropriação indevida de informação e está preparado para apoiar as organizações na gestão de crises relacionadas com falhas de segurança, cobrindo «custos de investigação, honorários jurídicos e monitorização de identidade das vítimas de violação de privacidade estão incluídos» (AIG, *CyberEdge*).

É ainda uma característica do produto a cobertura de eventuais perdas de lucros relacionadas com a interrupção do funcionamento dos sistemas informáticos, bem como, uma cobertura relativa a *cyber* extorsão.

6 CERTIFICAÇÕES EM CONTINUIDADE DE NEGÓCIO

6.1 Enquadramento da Norma ISO 22301

A ISO 22301 é uma norma internacional para a GCN que define os requisitos para que esta seja passível de ser auditada e certificada. Comunica para os clientes e outras partes interessadas a garantia que a organização está preparada para responder e recuperar em caso de disrupção, *IT Governance* (fevereiro, 2019).

De acordo com a ISO 22301 (2019 p. 0.1):

> *[t]his document specifies the structure and requirements for implementing and maintaining a business continuity management system (BCMS) that develops business continuity appropriate to the amount and type of impact that the organization may or may not accept following a disruption.*

Para as organizações que procurem certificação em matérias de continuidade de negócio, a ISO 22301 será a base daquilo que serão os planos elaborados e certificados por uma entidade isenta e capacitada para tal.

No *BCI Horizon Scan Report 2020* é possível constatar também que a adoção desta norma por parte das organizações tem vindo a crescer no último ano.

> *20.5% of respondents report their organization is certified to ISO 22301: an increase of 6.7 percentage points on 2018. 71.0% of organizations now get certified to the standard or use it as a framework – the highest percentage ever recorded in the Horizon Scan Report (BCI Horizon Scan Report 2020, p.6).*

A composição de um *Business Continuity Management System* (BCMS) de acordo com a ISO 22301 (2019 p. 0.1) passa pelo seguinte:

- *a policy;*
- *competent people with defined responsibilities;*
- *management processes relating to:*
    - *policy*
    - *planning*
    - *implementation and operation*
    - *performance assessment*
    - *management review*
    - *continual improvement*
- *documented information supporting operational control and enabling performance evaluation.*

6.2 Ciclo de Deming

No que se refere a modelos, a ISO 22301 (2012 p. V) apresenta-se sob um modelo conhecido por *Plan-Do-Check-Act* (PDCA), referindo-se como «*a model to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness at organization's BCMS*».

6.3 Considerações sobre a Norma 22301

Grande parte das organizações valorizam a norma ISO 22301 como uma importante fonte de informação sobre procedimentos e conceitos para as suas políticas de continuidade de negócio, no entanto apenas uma parte procura a certificação. De acordo com o *BCI Scan Report 2020* (p.34) «[t]*he primary reason given by 56.6% of respondents for not obtaining certification to ISO 22301 is due to no business requirement».*

Importa clarificar se as organizações que autonomamente desenvolvem as suas políticas de continuidade de negócio, sem necessidade da certificação, serão capazes de o fazer com a mesma robustez que as que são certificadas? Será que as orientações existentes para os setores que ainda não estão regulamentados nestas matérias, são uma forma de contribuir para a melhoria das práticas a nível global?

Para algumas organizações este panorama pode de facto não fazer sentido. No caso do setor bancário, a procura por uma certificação adicional quando o próprio setor já está fortemente regulamentado nestas matérias pode não fazer sentido. «*As mentioned previously, some organizations in regulated sectors felt it unnecessary to adhere to the standard due to having to comply to strict industry regulations» (*BCI Scan Report 2020, p.34).

> *We have our own internal audit function to carry out audits 3-4 times a year against what we say we're going to do in our business continuity program with reference to ISO 22301. We don't think that certification will add too much of an additional cost, but the bad thing for us would be the reputational risk of losing the certification. We therefore like the standard and use it to carry out audit measures against that, but we will not certify against it."«Business Continuity Manager, National Government, United Kingdom"* (BCI Scan Report 2020, p.35).

Existirá um risco acrescido para o mercado quando as organizações não procuram avaliações externas e independentes para as suas políticas de continuidade de negócio, sendo que assumidamente no relatório anteriormente referido, não o fazem em parte com receio de eventualmente perderem a certificação e mancharem a sua reputação?

6.4 Certificações DRII

Além da certificação ISO já referida, que abrange as políticas de continuidade de negócio de uma organização, existem organizações especialistas em *Business Continuity* e *Disaster Recovery* que formam e certificam profissionais e organizações nestas matérias.

As certificações em continuidade de negócio têm como objetivo dar um reconhecimento a nível global aos profissionais desta área e podem servir como uma segurança para as organizações, uma vez que tendo profissionais certificados nas empresas, o nível de confiança estabelecido nas suas políticas de continuidade de negócio deve aumentar.

Sendo de alguma forma fácil encontrar e pesquisar *online* diversas organizações que oferecem certificações em *Business Continuity* ou *Disaster Recovery,* no decorrer da presente investigação e nos exemplos dados em seguida são consideradas apenas duas organizações, tidas como das mais relevantes a nível mundial e utilizadas noutros pontos como fontes para este projeto.

O *Disaster Recovery Institute International* (DRII) é o mais antigo instituto a fornecer apoio às empresas a nível mundial em matérias de continuidade de negócio e recuperação de desastre, através de formações e certificações. Esta organização está sediada no Estados Unidos da América e está também representada na Europa em Londres. Tem também presença noutros locais através de filiais autorizadas que representam a organização.

Em Portugal, as formações e as certificações do DRII, à data da elaboração da presente investigação, são representadas pela empresa Behaviour - Formação e Consultoria, Lda com sede em Lisboa.

Na consulta à página da Internet do DRII, é possível verificar certificações em duas grandes áreas; certificações de indivíduos e certificações de organizações.

No âmbito da certificação de organizações, o processo de aprovação da certificação *Center of Excellence in Resilience* disponível na página do DRII, ocorre da seguinte forma:

> *[a]n extensive approval process and qualifying protocols help to ensure the appropriate level of knowledge and proficiency of an entity's BCM program; including an onsite inspection of the company, credentials, ethical practices, and BCM training records/documentation, followed by an interview. Each assessment team will be led by an ANSI [American National Standards Institute] accredited examiner and a Certified Business Continuity Lead Auditor (CBCLA) who has extensive audit experience.*

O DRII disponibiliza ainda várias áreas de certificação em continuidade de negócio para indivíduos, nomeadamente certificações em:

- *Continuity;*
- *Advanced Continuity;*
- *Vendor ;*
- *Audit;*
- *Cyber Resilience;*
- *Healthcare Continuity;*
- *Public Sector Continuity;*
- *Risk Management;*

Detalhando os dois tipos de certificação relacionadas com auditoria, é disponibilizada a possibilidade de obter *Certified Business Continuity Auditor* detalhado na página do DRII como:

> *specialist who can verify the effectiveness of an organization's business continuity program against the landscape of standards, guidelines and industry regulations. Internally or externally, the CBCA demonstrates an ability to validate and evaluate plans based on any applicable standard.*

A outra certificação, a um nível individual e que é também disponibilizada pelo DRII é a de *Certified Business Continuity Lead Auditor* detalhada no sítio Internet à data da consulta como:

> *a professional certification for audit team leaders. The requirements to be a CBCLA reflect significant audit experience as well as extensive understanding in emergency management, enterprise risk management and business continuity. Those who have been responsible for planning, scheduling and implementing an audit program are excellent candidates for CBCLA.*

6.5 Certificações BCI

O *Business Continuity Institute* (BCI) é uma organização sediada no Reino Unido e presente a nível global cujo âmbito da atividade é a continuidade de negócio e resiliência das organizações. Através de formações, certificações e partilha das melhores práticas sobre continuidade de negócio, o BCI apoia os indivíduos e as organizações a serem mais resilientes perante eventuais adversidades.

O BCI disponibiliza a possibilidade de obter o *Certificate of the Business Continuity Institute* (CBCI) como uma forma de provar ao mercado conhecimento e construir uma rede de contactos a nível global sobre resiliência e continuidade de negócio.

De acordo com a página de Internet do BCI à data da consulta:

> *[t]he CBCI Certification Course is the BCI's number one course that teaches you the fundamentals to implement a Business Continuity Management (BCM) programme into your organization and provides you with a solid base for a career in business continuity and resilience.*

Esta certificação abrange conteúdos desde meros introdutórios da continuidade de negócio, a como desenvolver, implementar e manter as políticas de gestão de continuidade de negócio, bem como, informação sobre as melhores práticas do mercado. Para as organizações, o BCI oferece a possibilidade de *Corporate Partnership* como um apoio para as organizações se tornarem mais resilientes. Ainda de acordo com a página Internet do BCI à data da consulta, é referido sobre *Corporate Partnership*, o seguinte:

> *[b]y empowering all staff, not just those responsible for business continuity, with basic awareness and knowledge it will help your organization if a crisis or incident occurs, helping you to recover quicker and save time and money. It also demonstrates to stakeholders your commitment to business continuity and resilience.*

Figura 6.1 Grupos de empresas clientes *Corporate Membership* do BCI

Fonte *BCI Corporate Membership*

7 AUDITORIA A SGCN

7.1 GCN como Matéria Auditável

Recorrendo ao modelo de GCN disponibilizado pela ISO 22301 podemos verificar como parte da avaliação do desempenho do sistema implementado, a existência de Auditorias Internas. Sobre este tema, a ISO 22301 (2019, p. 9.2.2) refere que as organizações devem:

- Planear, implementar e manter programas de auditoria que incluam a frequência, métodos, responsabilidades, requisitos de planeamento e *reporting*, que deverão ter em consideração a importância dos processos e das auditorias anteriores;
- Definir os critérios das auditorias e a sua abrangência;
- Selecionar os auditores e conduzir as auditorias de forma a garantir a sua objetividade e independência no processo de auditoria;
- Garantir que os resultados das auditorias são reportados às chefias que interessam;
- Manter documentadas evidências da implementação de programas de auditoria e os seus resultados;
- Garantir que quaisquer medidas corretivas são aplicadas sem que sejam eliminadas inconformidades detetadas, bem como, as suas causas;
- Garantir que o *follow-up* das auditorias inclui a verificação das medidas tomadas e quais os resultados da verificação feita.

Neste sentido, o *Institute of Internal Auditors* (IIA) define auditoria interna como:

> auditoria interna é uma atividade independente, de garantia e de consultoria, destinada a acrescentar valor e a melhorar as operações de uma organização. Assiste a organização na consecução dos seus objetivos, através de uma abordagem sistemática e disciplinada, para a avaliação e melhoria da eficácia dos processos de gestão de risco, controlo e governação.

Cabe a cada organização como forma de controlo interno e melhoria contínua, desenvolver auditorias internas robustas e abrangentes o suficiente de forma a que a administração, a quem por norma reporta a auditoria, tenha conhecimento da forma como funcionam as diferentes áreas, face ao que está planeado.

De acordo com CMVM *et al* (2010, p7) «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».

7.2 Importância da Auditoria a PCN

Swanson (2013) indica que auditorias internas à segurança dos SI, PCN e PRD, são altamente recomendadas. A gestão de topo / administração deve garantir que, efetivamente, os planos estão preparados para serem colocados em prática em qualquer momento e que a continuidade das operações está assegurada de forma eficaz e eficiente.

Uma análise independente dos PCN ou de recuperação de desastre por parte dos auditores internos pode fornecer informações objetivas sobre a adequação dos programas para prevenirem a não continuidade do negócio em caso de falhas. Os PCN devem ser atualizados ao mesmo ritmo da evolução do meio envolvente da organização (Swanson, 2013).

Como noutras matérias, a auditoria a PCN é uma função essencial de garantia e obtenção de prova de conformidade dos processos face ao definido inicialmente como objetivo. Bronack (2012), indica que uma auditoria a PCN no âmbito dos SI é essencial e verifica os seguintes aspetos:

- A adequação nível de abrangência do plano;
- A disponibilidade dos processos e pessoas para implementar do plano;
- Os testes efetuados;
- A verificação das funções diárias necessárias para que o plano possa ser posto em prática, a qualquer momento e de forma eficaz;

Bronack divide a auditoria a PCN em três grandes componentes:

- Validação do PCN;
- Identificação e validação de medidas preventivas e que visem facilitar a continuidade;
- Análise das evidências sobre o desempenho das atividades que garantem a continuidade e recuperação;

7.3 Auditoria Interna

A auditoria interna será fundamental para as organizações que disponham de um SGCN pois esta função irá trazer um determinado grau de confiança nas políticas existentes, essencial para a manutenção do normal funcionamento destes planos. Ao longo da presente investigação, procura-se demonstrar a evidência que a auditoria interna irá desempenhar importantes funções, quer nas organizações inseridas em setores regulamentados, quer nas organizações que procuram obter certificações nestas matérias.

Levanta-se assim a questão se as restantes organizações não influenciadas por regulamentações ou certificações, têm como prática a realização de auditorias sobre matérias de continuidade de negócio. E ainda, se a não realização destes trabalhos pode trazer eventuais consequências negativas não só para as organizações, mas para todo o mercado?

A auditoria interna será um processo desempenhado por uma equipa independente tendo por base documentos na procura de evidências de que as matérias de continuidade de negócio estão em conformidade com os critérios definidos para a auditoria. «Os processos de continuidade de negócio podem ser considerados eficientes quando os resultados indicam que há um processo estruturado de auditoria interna». (Manoel S.S, 2019, p.292).

Em parte, será a partir dos resultados desta auditoria interna que a administração irá fazer a sua revisão das políticas de gestão de continuidade e determinar se existem ou não ações a serem tomadas num sentido de correção ou melhoria.

Deve existir um plano de auditoria na organização que defina a regularidade das auditorias a acontecerem, bem como, um responsável pelos trabalhos realizados. Como para outras matérias auditáveis pode não existir alguém nas equipas de auditoria com conhecimentos para desempenhar as funções necessárias e nesse caso deve ser nomeado alguém com experiência nestes assuntos para fazer parte dos trabalhos (Manoel S.S, 2019, p.292).

O autor refere ainda neste seguimento, que no plano de auditoria podem estar incluídos os seguintes aspetos:

- Objetivos para o plano de auditoria e auditorias individuais;
- Abrangência/número/tipos/duração/ localizações/programação de auditorias;
- Procedimentos do plano de auditoria;
- Critérios de auditoria;
- Métodos de auditoria;
- Seleção das equipas de auditoria;
- Recursos necessários, incluindo viagens e alojamento;
- Processos para tratamento da confidencialidade, segurança da informação, saúde, segurança e outros assuntos similares.

As figuras 7.1 e 7.2 apresentadas de seguida exemplificam de uma forma genérica uma lista de verificação de conformidade de processos auditados.

Exemplo de lista de verificação de conformidade num processo de auditoria.				
Requisitos	**Fonte**	**Conformidade SIM ou Não**	**Evidências**	**Observações**
Requisito A	Documentação interna relacionada com Requisito A		Estão documentados os trabalhos relacionados com o requisito A	
Requisito B	Confirmação externa relacionada com Requisito B		Entidade externa confirmou condições relacionados com Requisito B	
Requisito C	Resultado de avaliações relacionadas com Requisito C		Avaliações foram positivas relativamente ao Requisito C	

Figura 7.1 Exemplo de lista de verificação de conformidade num processo de auditoria

Fonte autoria própria

EXEMPLO DE LISTA DE VERIFICAÇÃO – Processo auditado – Recursos Humanos				
Requisito da ABNT NBR ISO 22301	**Fonte**	**Conformidade SIM ou NÃO**	**Evidências (buscar)**	**Observação**
Cláusula 4 – Contexto	Análise do contexto interno da organização Quais responsabilidades dos requisitos legais		Qual foi a saída da análise de contexto e como isso impacta o RH? De quais requisitos legais o RH deveria estar ciente no evento do incidente?	
Cláusula 5 – Liderança	Política de Continuidade de Negócios		Como o RH está cumprindo as responsabilidades das Políticas?	
Cláusula 8.2.2 Análise de impacto no negócio	Documento com os resultados da Análise de Impacto no Negócio		Como o RH vai alocar pessoas suficientes para voltar à normalidade em apenas os dias descritos no RTO?	
8.2.3 Processo de avaliação de riscos	Resultados do processo de avaliação de riscos		Qual é o apetite aos riscos da organização e como isso afeta o papel do RH?	

Figura 7.2 Exemplo de lista de verificação de um processo auditado

Fonte Manoel S.S (2019, p.297)

De acordo com Swanson (2013), uma auditoria interna a PCN pode incluir, além de outros, os seguintes testes:

- Entrevistas aos principais *Stakeholders* e participantes dos programas de continuidade;
- Revisão da documentação do projeto, o seu planeamento e outros documentos relacionados com TI;
- Revisão dos planos através da verificação que estes são completos, apropriados e atualizados;
- Verificação dos tempos de recuperação e obtenção de prova de que são possíveis de atingir;
- Examinação da informação obtida nos testes efetuados, procedimentos e comunicações por parte da gestão referentes a situações de BCP ou DR que possam ocorrer e o que os colaboradores devem fazer;
- Revisão dos planos de testes a efetuar e dos resultados dos testes já efetuados;
- Avaliação dos funcionários mais relevantes quanto à sua preparação e conhecimento dos procedimentos;
- Revisão do impacto que novas leis ou regulamentos possam ter nos planos;
- Revisão de contratos e prontidão dos serviços relacionados.

7.4 Auditoria como Base para a Certificação

O trabalho de auditoria, conforme já referido, tem um papel importante como garantia de conformidade do planeamento de continuidade de negócio face ao que são os requisitos das organizações ou dos modelos a serem aplicados.

Manoel S.S (2019, p.66) detalha os passos mais comuns para a certificação da norma ISO 22301, adaptada para o Brasil, da seguinte forma:

- Implementação do sistema de gestão de continuidade de negócio;
- Auditoria interna e análise critica da gestão de topo;
- Seleção do organismo de certificação;
- Auditoria de pré-avaliação (opcional);
- Auditoria fase 1 e auditoria de fase 2;
- Auditoria de acompanhamento (opcional);
- Confirmação do registo;
- Auditorias contínuas de melhoria e vigilância.

Segundo o autor, antes de existir a primeira auditoria, o sistema de gestão de continuidade de negócio já deve estar implementado, só assim dando lugar à primeira auditoria que será interna e que valida deste modo a preparação para a procura de certificação.

A auditoria de pré-avaliação será uma auditoria opcional que pretende «identificar qualquer lacuna possível entre o seu SGCN e os requisitos da Norma» (Manoel S.S 2019, p.67).

A auditoria caracterizada como fase 1, terá como objetivo a verificação da conformidade entre os requisitos da norma, os objetivos da organização e o sistema implementado pela organização.

A auditoria de fase 2 de acordo com o autor, diferencia-se da primeira por adicionar a verificação de que o planeado está de facto implementado na organização e se tem a capacidade de ajudar a organização a atingir os seus objetivos, mantendo sempre presente os requisitos da norma.

Quanto à auditoria de acompanhamento, sendo esta uma fase opcional, aplica-se no caso de existirem não conformidades e em que seja solicitada uma validação das medidas tomadas neste sentido.

Por fim é referida a auditoria de acompanhamento e vigilância que será executada pela entidade certificadora e visa garantir que continua a existir conformidade com a norma e os objetivos da organização, havendo espaço para a introdução de melhorias. O autor neste caso faz referência a uma periodicidade de pelo menos um ano (Manoel S.S 2019, p.67).

O modelo acima referido é detalhado quanto aos diferentes processos de auditoria. Serve apenas como exemplo de uma forma de trabalho. Existem decerto formas diferentes, mas o importante é a utilização de boas práticas, com o intuito de demonstrar a importância da auditora aos SGCN na procura de certificação.

8 COMPONENTE EMPÍRICA

8.1 Entrevistas realizadas

Numa fase inicial da investigação e no âmbito do que foi considerada a componente empírica do presente trabalho, foi desenvolvido um conjunto de questões disponibilizadas no Anexo 3, que levantavam algumas das dúvidas principais sobre o tema. Estas questões foram utilizadas em duas entrevistas realizadas e que tiveram como objetivo a validação da pertinência das mesmas bem como retirar algumas considerações importantes sobre o tema, que são expostas de seguida.

Relativamente às entrevistas realizadas uma delas foi feita com um diretor de Risco Operacional de uma instituição financeira, um banco que atua no mercado português. Trata-se de um contacto de grande importância para a investigação desenvolvida, uma vez que pertence a uma área fortemente regulamentada e auditada, sendo a componente de continuidade de negócio um dos fatores críticos objeto de regulamentação existente.

A segunda entrevista foi realizada com um diretor de segurança a nível nacional de uma empresa líder na área da logística a atuar no mercado ibérico.

Uma das primeiras questões abordadas centrou-se no tema da diferenciação dos conceitos de continuidade de negócio e recuperação de desastre. Ao longo da investigação realizada no âmbito da dissertação, embora as principais fontes façam uma clara distinção entre uma matéria e outra, por vezes até são referidos departamentos que em teoria estão separados, para que esta distinção possa ser feita em termos operacionais, as organizações precisam de ter uma estrutura desenvolvida o suficiente para que possa suportar esta separação.

Foi então necessário questionar se estas organizações, consideradas empresas com notoriedade no nosso mercado, fazem de facto esta distinção. No caso da organização que representa o setor bancário não existe uma separação entre as duas funções, nem sequer um departamento exclusivamente responsável pela continuidade de negócio, uma vez que esta é uma responsabilidade do departamento de risco operacional.

No entanto, provavelmente por força das regulamentações e auditorias, os processos definidos estão de acordo com esta diferenciação e talvez apenas por uma questão de dimensão não existam pessoas a trabalhar exclusivamente nestes assuntos.

Esta diferenciação é possível de verificar, pois existem três cenários possíveis de desastre para os quais a organização está preparada, sendo eles, desastre físico (incêndio, terramoto, inundação, entre outros), cenário de uma pandemia (vírus ou outras doenças contagiosas que ponham em causa a integridade dos colaboradores) e o cenário de desastre tecnológico (ataque informático ou falha dos sistemas). Desta forma podemos constatar os dois primeiros cenários no âmbito de PCN e o último mais numa vertente de PRD.

No caso da empresa pertencente à área logística, a resposta obtida foi mais clara, tendo sido dada a indicação que esta separação não tem de existir necessariamente e que estas duas matérias são indissociáveis.

Possivelmente por este último setor por não ser regulamentado e em princípio a organização não ser auditada nestas matérias, não exista uma maior conformidade com a distinção apresentada pelas principais referências bibliográficas.

Outra questão considerada relevante para o estudo foi o envolvimento da gestão de topo / administração na elaboração e testes efetuados no âmbito da continuidade de negócio. Sobre este tema existe conformidade nas respostas, na medida em que os decisores máximos da organização devem aprovar os planos elaborados e por isso estarem envolvidos nos mesmos.

O tema da certificação ISO 22301 foi outro dos assuntos abordados. Foi consensual a importância desta certificação, ou qualquer outra que influencie as organizações a ter presente a importância dos processos definidos nos planos e dos testes regulares a serem efetuados. Por norma a pressão de auditorias ou de necessidade de apresentar certificações a terceiros, é o que leva as organizações a estarem melhor preparadas para estes eventos.

Um dos fatores apresentados com importantes no desenvolvimento dos PCN ou PRD são as medidas alternativas para eventuais eventos disruptivos em terceiros, cujos serviços sejam essenciais para a organização. Por exemplo, na eventualidade de falha de algum dos principais fornecedores, é importante que a organização esteja preparada para continuar. Este é um ponto que foi consensual nos entrevistados. Uma das soluções apresentadas e que está em prática, passa pela existência de cláusulas de continuidade nos contratos com fornecedores.

Em seguimento, foi abordada a questão da hierarquização dos fornecedores por ordem de importância a constar nos planos a serem desenvolvidos. Embora todos os fornecedores sejam importantes, certamente existe uma parte deles que é facilmente substituída em qualquer altura, mesmo não se tratando de algum evento disruptivo. Outros eventualmente serão mais exclusivos, desta forma importa que existam planos bem definidos para alternativas em caso de necessidade.

Uma consideração importante que foi retirada é de que esta hierarquização não deve ser abordada por uma mera observação dos fornecedores, mas sim dos processos cruciais da organização e por sua vez, quais são os fornecedores envolvidos nestes processos.

A regularidade dos testes foi outro dos assuntos mitigados. É possível considerar que os testes devem realmente ser efetuados, pelo menos, numa base anual. Esta base temporal não significa que seja feito, por exemplo, um simulacro por ano, mas sim um evento simulado em termos anuais para cada cenário chave contemplado no plano.

No caso da instituição financeira que tem vários cenários, não é possível testar num único dia todas as possibilidades, podendo estas simulações durarem vários dias, semanas, ou serem repartidos por fases ao longo do ano. Este é um tema que dependerá sempre da complexidade dos planos, bem como, da capacidade que a estrutura da organização tem para suportar estes testes. Uma organização considerada resiliente deverá ter documentadas as evidencias dessa resiliência e este será um dos pontos sobre onde devem incidir as auditorias.

Quanto ao envolvimento e conhecimento sobre os planos de todas as pessoas da organização, foi possível observar um grau de maturidade diferente nas respostas das organizações em análise.

Enquanto a organização na área logística indica claramente que apenas as pessoas consideradas chave estão envolvidas, a instituição financeira, embora tenha também um grupo de pessoas chave e com funções mais especificas, indica que todas as pessoas devem ter conhecimento dos planos e da sua missão no caso da ativação dos mesmos.

8.2 Enquadramento do Questionário

Ainda no âmbito da componente empírica do presente trabalho foi desenvolvido um questionário que foi distribuído a profissionais com experiência em matérias de continuidade de negócio, com o objetivo de através da amostra possível verificar quais as práticas mais comuns.

Adicionalmente foram obtidas algumas opiniões sobre os diversos assuntos abordados no questionário através de comentários deixados pelos inquiridos ao responderem às questões. Estas opiniões foram utilizadas para que se possam tecer algumas considerações relevantes além das respostas diretas às diversas questões.

O questionário foi desenvolvido com o apoio do, à data, *Chief Information Security Officer* (CISO) do Gabinete Nacional de Segurança, Sr. Tenente-Coronel Agostinho Valente, que com a sua experiência em matérias relacionadas com continuidade de negócio e certificação nesta área, deu um importante contributo na definição de um questionário que abordasse os assuntos mais essenciais sobre a continuidade de negócio.

Uma das primeiras dificuldades encontradas inicialmente, foi a disponibilidade dos inquiridos em falar sobre assuntos que são considerados sensíveis para as organizações, tendo o anonimato das respostas sido a solução encontrada para facilitar chegar à amostra final.

O questionário inicial e de elaboração própria era composto por 6 questões iniciais de caracterização da amostra e 25 questões abertas sobre o tema continuidade negócio. Este questionário foi utilizado em duas entrevistas realizadas com o objetivo de validar o conteúdo das questões e eventualmente encontrar junto dos profissionais em questão assuntos que pudessem estar em falta abordar no questionário.

As realizações das entrevistas referidas anteriormente serviram além das conclusões já apresentadas, para validar o conteúdo das questões que serviram de base para a formação do questionário final.

Ao ter sido estabelecido o contato com o Sr. Tenente-Coronel Agostinho Valente foi apresentado o questionário inicial referido anteriormente bem como a dificuldade até então em encontrar profissionais com experiência nestas matérias dispostos a contribuir para o estudo.

Uma das recomendações feitas e que foi considerada foi a redução do número de questões sobre continuidade de negócio, passando assim o questionário a manter 6 questões de caracterização, mas reduzindo para 13 o número de questões sobre continuidade de negócio.

Este foi um ponto essencial para tornar o questionário menos extenso e mais *friendly*, possibilitando a obtenção de um número de respostas maior que o que estava a acontecer inicialmente.

As questões principais sobre o tema continuidade de negócio foram elaboradas de forma a que as respostas pudessem ser de Sim ou Não, havendo no entanto espaço para comentários com o intuito de eventualmente surgirem recomendações, conclusões ou explicações sobre os diversos assuntos.

Este questionário final foi elaborado e distribuído através da plataforma *online* e gratuita para as suas funções mais básicas, Survio.

Quanto à distribuição do questionário esta foi feita através da partilha do link com diversos contactos a nível pessoal e profissional que foram surgindo de indivíduos com experiência. Por sua vez os contactos estabelecidos foram sugerindo novos contactos ou passando o questionário a colegas com experiência nestas mesmas matérias.

O número final de respostas validadas e a partir do qual os dados foram trabalhados foi de 36 respostas.

8.3 Resultados do Questionário Final

8.3.1 Questão 1. Qual é o tipo de organização (Pública, Privada, Terceiro Setor) onde trabalha?

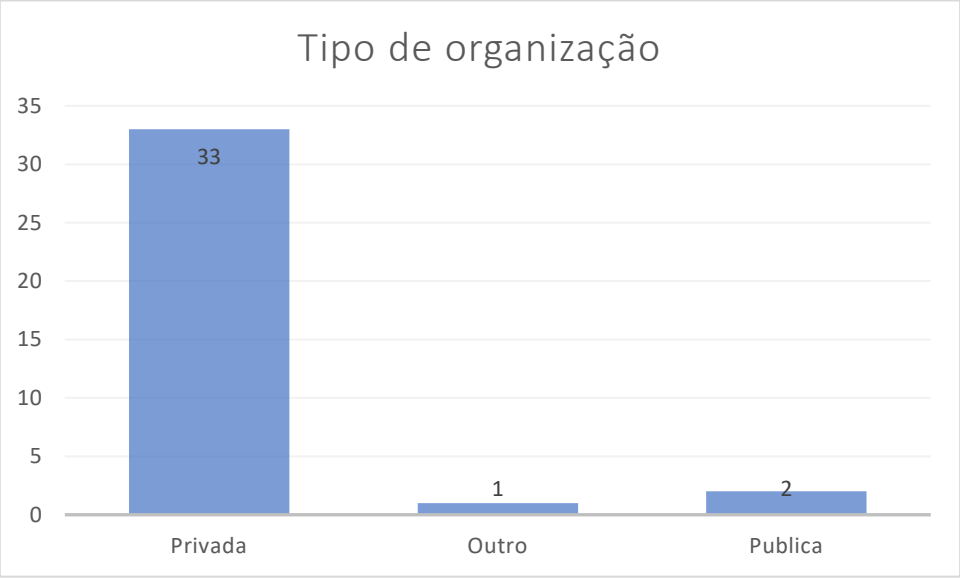

Figura 8.1 Tipo de organização.

Fonte elaboração própria

A amostra obtida é predominantemente de pessoas que trabalham em organizações privadas, sendo das 36 respostas totais apenas 2 do setor publico e 1 classificada como de outro tipo, por se tratar de uma IPSS.

8.3.2 Questão 2. Qual é o setor de atividade da organização onde presta as atuais funções?

Figura 8.2 Setor de atividade

Fonte elaboração própria

Tendo sido tomada a opção de as respostas serem livres, ocorrem algumas situações em a resposta não se enquadra exatamente com aquilo que é esperado. Por exemplo as respostas classificadas como n/a foram respostas em que foi dito em que departamento da própria organização desempenhavam funções, quando o objetivo seria o setor em que a empresa se enquadra.

Algumas classificações não são necessariamente indissociáveis, por exemplo seria possível classificar as organizações do setor financeiro e de consultoria como serviços. No entanto a experiência inicial de contacto com profissionais da área foi que nem todos estavam dispostos a indicar o mínimo de informação que pudesse ajudar a identificar as organizações. Por este motivo foi dada a liberdade de que conforme se sentissem mais confortáveis detalhassem mais as suas respostas.

O número de respostas obtidas no setor financeiro, em que inclui as respostas de banca e seguros, é sem dúvida uma forte contribuição para o presente trabalho uma vez que se trata de um setor regulado em termos de políticas de continuidade de negócio.

Esta característica da amostra permite assim a diversificação com entidades não reguladas, tornando os resultados menos influenciados por este fator.

8.3.3 Questão 3. Qual é o cargo/posição que ocupa na organização?

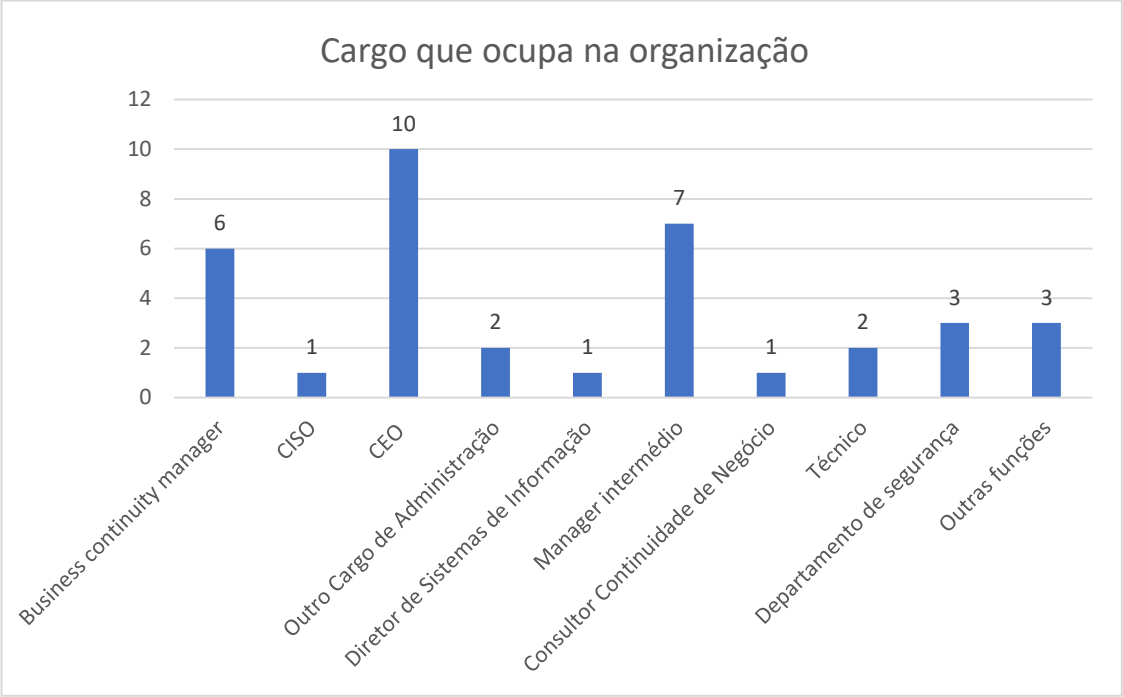

Figura 8.3 Cargo que ocupa na organização

Fonte elaboração própria

A terceira questão pretende apurar o cargo desempenhado pela pessoa que está a responder ao questionário, tendo neste aspeto a amostra superado as expectativas iniciais de um número inferior de cargos de chefia e diretamente relacionados com a continuidade de negócio.

A destacar das 36 respostas apenas 2 classificadas como técnicos e 3 em outras funções não relacionadas diretamente continuidade de negócio.

Embora estas outras funções pudessem à partida ser um fator que invalidasse a resposta por puderem não ter conhecimento suficiente sobre os assuntos abordados, os questionários foram apenas passados a pessoas com experiência em continuidade de negócio ou em cargos de chefia/ administração.

Significa isto que terão respondido ao questionário por indicação de alguém com experiência nestes assuntos ou em cargos de chefia/ administração de organizações, tendo por isso as respostas sido consideradas válidas.

8.3.4 Questão 4. Qual é o número total de empregados?

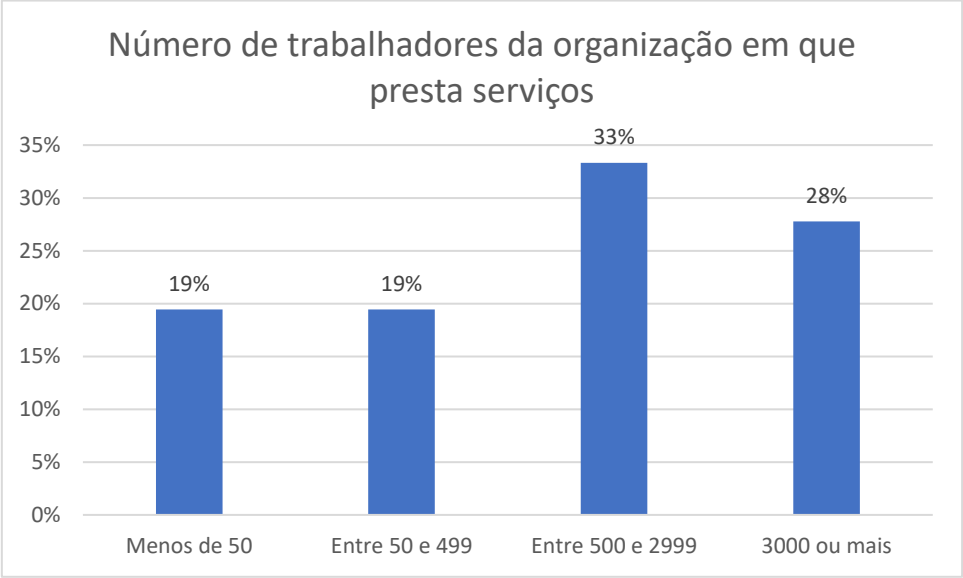

Figura 8.4 Número de trabalhadores da organização em que presta serviços

Fonte elaboração própria

O número total de trabalhadores permite ter uma noção da dimensão das organizações para as quais prestam serviços os inquiridos, sendo que, conforme foi referido ao longo do trabalho, a dimensão das organizações é um fator condicionante das políticas de continuidade de negócio.

Os intervalos utilizados foram feitos com base na Recomendação Da Comissão de 6 de Maio de 2003 relativa à definição de micro, pequenas e médias empresas, publicada no Jornal Oficial da União Europeia, bem como com base no Decreto-Lei n.º 81/2017 que é uma alteração à definição publicada inicialmente.

Do total de 36 respostas obtidas 7 indicam menos de 50 trabalhadores, 7 entre 50 e 499, 12 respostas entre 500 e 2999 e as restantes 10 indicam 3000 ou mais trabalhadores.

Na redação inicial relativa à definição de micro, pequenas e médias empresas com alteração posterior em 2017 são consideradas no Artigo 2º, Nº2 como pequenas empresas as que empregam menos do que 50 pessoas.

Esta definição desaparece com a alteração introduzida em 2017, no entanto é utilizada no âmbito deste trabalho por ser considerado importante haver alguma distinção entre as diferentes organizações até 499 trabalhadores.

No Decreto-Lei n.º 81/2017 no Nº3 dos Artigo 2º são definidas como empresas de pequena média capitalização, as que têm menos de 500 trabalhadores, e no N.º 2 do mesmo Artigo, consideradas de média capitalização as que não tendo menos de 500 trabalhadores tenham menos de 3000 trabalhadores.

8.3.5 Questão 5. Em que ano a organização foi constituída?

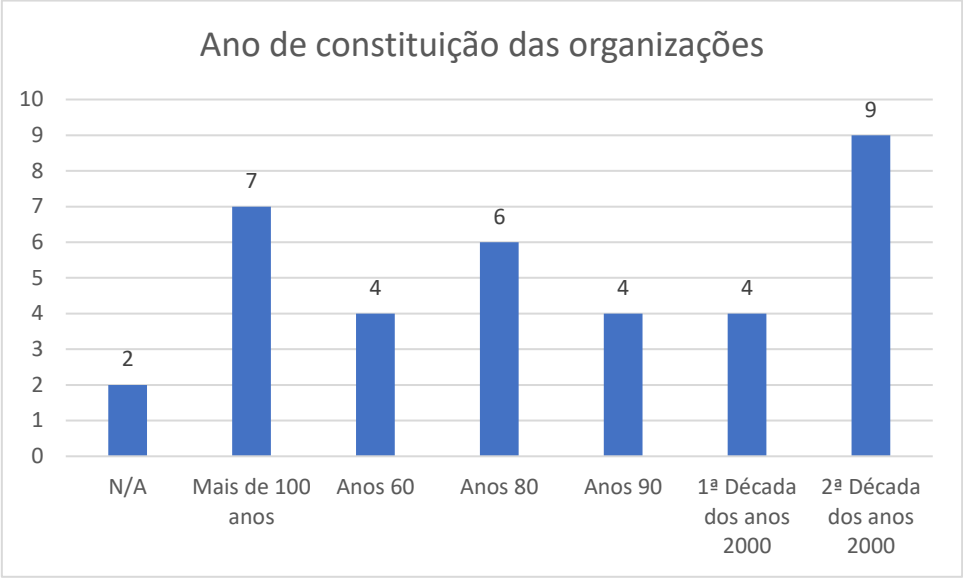

Figura 8.5 Ano de constituição das organizações

Fonte elaboração própria

A quinta pergunta ainda numa ótica de caracterização da amostra pretende identificar a antiguidade das organizações para as quais prestam serviços os inquiridos.

Com esta questão pretende-se comprovar a diversidade entre organizações com uma longa história de atividade e outras organizações mais recentes que provavelmente ainda estão a definir o seu negócio e a estabelecer-se no mercado.

Duas das respostas obtidas não foram consideradas válidas para esta questão uma vez que não especificaram exatamente o ano de formação não tendo por isso sido possível tirar conclusões neste sentido.

Das 34 respostas validadas para esta questão 13 são de organizações que iniciaram atividade durante ou após o ano 2000, sendo que destas 9 terão mesmo iniciado na segunda década dos anos 2000. Desta forma temos um número expressivo, face à amostra, de empresas que à data da resposta ainda não terão atingido os 10 anos de atividade.

Existe por isso uma diversificação nas respostas de empresas que dada a sua pouca antiguidade se podem considerar menos experientes no mercado e empresas com mais experiência de negócio, considerando assim que as respostas não são tendencialmente influenciadas por se tratarem apenas de organizações exclusivamente com mais experiencia ou menos experiencia.

8.3.6 Questão 6. A quem reporta na organização?

Figura 8.6 A quem reporta na organização

Fonte elaboração própria

A sexta questão teve com objetivo compreender se as pessoas que estavam a responder ao questionário se encontram próximas da administração ou diretores de áreas que possam ter a cargo partes importantes das políticas de continuidade de negócio.

Das 36 respostas obtidas 2 não especificaram exatamente a função pelo que foram classificadas como n/a.

A classificação em diretor de área é a que acaba por ser menos conclusiva quanto ao seu significado. Tendo as perguntas sido de resposta aberta para esta parte dos inquiridos fez sentido responder que reportavam ao diretor da área ou do departamento, o que não permite concluir exatamente sobre a proximidade à administração ou cargos que por norma estejam envolvidos na continuidade de negócio.

As restantes respostas foram consideradas bastante satisfatórias quanto à proximidade com a administração ou cargos que por norma assumem responsabilidade sobre as políticas de continuidade de negócio, sendo certamente uma mais valia para a qualidade das respostas.

8.3.7 Questão 7. Qual é o cargo desempenhado pela pessoa responsável pelo Plano de Continuidade de Negócio e a que nível está na organização? (Estratégico, Tático ou Operacional)

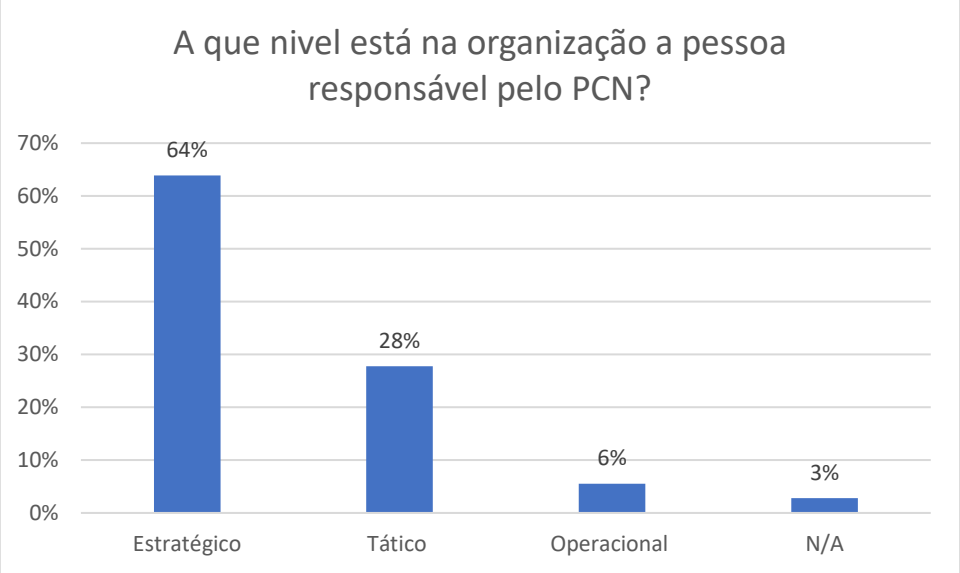

Figura 8.7 A que nível está na organização a pessoa responsável pelo PCN?

Fonte elaboração própria

A sétima questão e a primeira, após a caracterização da amostra pretende compreender junto dos inquiridos a que nível na organização desempenha funções a pessoa responsável pelos PCN bem como que cargo desempenha.

Das respostas obtidas 23 referem ser ao nível estratégico que está a responsabilidade pelo PCN, 10 a um nível mais tático, 2 a nível operacional e 1 resposta foi dada como "n/a".

Como foi referido ao longo do trabalho os modelos mais robustos de aplicação de políticas de continuidade de negócio colocam estas mesmas políticas como uma preocupação que se deve posicionar ao nível estratégico das organizações, de forma a que exista um fluxo de cima para baixo a nível hierárquico da cultura de continuidade de negócio.

Conforme observado pelas respostas a maioria das organizações têm ao nível estratégico a responsabilidade pelos PCN o que pode levar a entender que esta prática é comum.

Uma das vantagens observadas pelo questionário ser de resposta aberta é a possibilidade de analisar alguns comentários adicionais aos assuntos tratados pelas perguntas. No caso da questão em análise neste ponto é de relevar um comentário aparentemente de alguém ligado a consultoria na área de continuidade de negócio, onde refere que o que observa ser mais comum nos seus clientes é a pessoa responsável desempenhar funções ao nível da segurança, e (sendo este o ponto considerado mais interessante do comentário) que em organizações mais pequenas por norma é do diretor de IT que é responsável por um DRP.

Esta observação é uma clara demonstração do impacto que a dimensão das organizações tem na forma como se estruturam as políticas de continuidade de negócio, e que em organizações mais pequenas se vê por norma a preocupação apenas ao nível de IT.

Entre as diversas respostas os cargos desempenhados pelas pessoas responsáveis pelos PCN identificados na amostra obtida são cargos de administração, CEO, IT *business manager,* direção de qualidade, *manager* de *compliance,* gestor de continuidade de negócio ou direção de risco.

Verifica-se pela diversidade de cargos, que a função de responsável pelos PCN não é, pelo menos na amostra obtida, algo padronizado e que cada organização acaba por definir de acordo com a sua realidade.

8.3.8 Questão 8. A administração/gestão de topo está altamente envolvida na elaboração e testes dos Planos de Continuidade de Negócio?

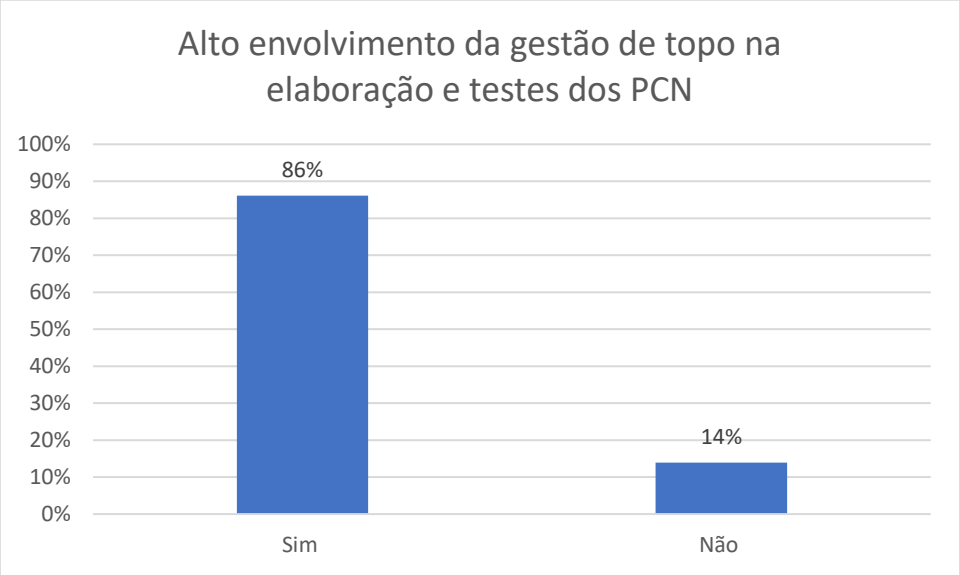

Figura 8.8 Alto envolvimento da gestão de topo na elaboração e testes dos PCN

Fonte elaboração própria

Quanto ao alto envolvimento da gestão de topo nas políticas de continuidade de negócio, a grande maioria das respostas apontam para que esta se encontra altamente envolvida, tendo 31 respondido positivamente à questão enquanto apenas 5 responderam que não. Isto significa que esta prática é comum e aplicada pelas organizações.

No entanto dada a possibilidade de analisar alguns comentários sobre este tema, para os inquiridos que decidiram adicionar mais algum contributo é possível observar que a políticas embora existam possam não espelhar exatamente aquilo que se passa nas organizações.

Duas das respostas positivas quanto ao envolvimento da gestão de topo deixaram, no entanto, o comentário de que existe envolvimento porque a gestão de topo deve aprovar os planos por questões de *compliance*.

A existência das aprovações por parte da gestão de topo, por si só já atribuem assim a responsabilidade ao mais alto nível dentro da organização, no entanto deixam na dúvida se existirá envolvimento de facto e acompanhamento, ou se passam apenas por aprovações dos trabalhos realizados.

Numa das respostas consideradas negativas é indicado que existe comprometimento da gestão de topo, mas que, no entanto, não está envolvida diretamente e que tanto a elaboração como os testes são realizados por um departamento de risco.

Apenas com alguma investigação mais aprofundada dos casos em específico se poderia perceber se das duas respostas consideradas positivas no parágrafo anterior, não poderiam estar a indicar o mesmo que esta referida agora, e considerada negativa.

Noutra nota deixada numa das respostas é referido que na observação de várias empresas clientes é possível perceber que a perceção da importância dos PCN tem vindo a aumentar e por isso também o envolvimento da administração de topo tem vindo a crescer tornando este tema cada vez mais uma prioridade.

8.3.9 Questão 9. Existe algum tipo de certificação ao nível da Continuidade de Negócio e/ou pessoas envolvidas e certificadas nestas matérias?

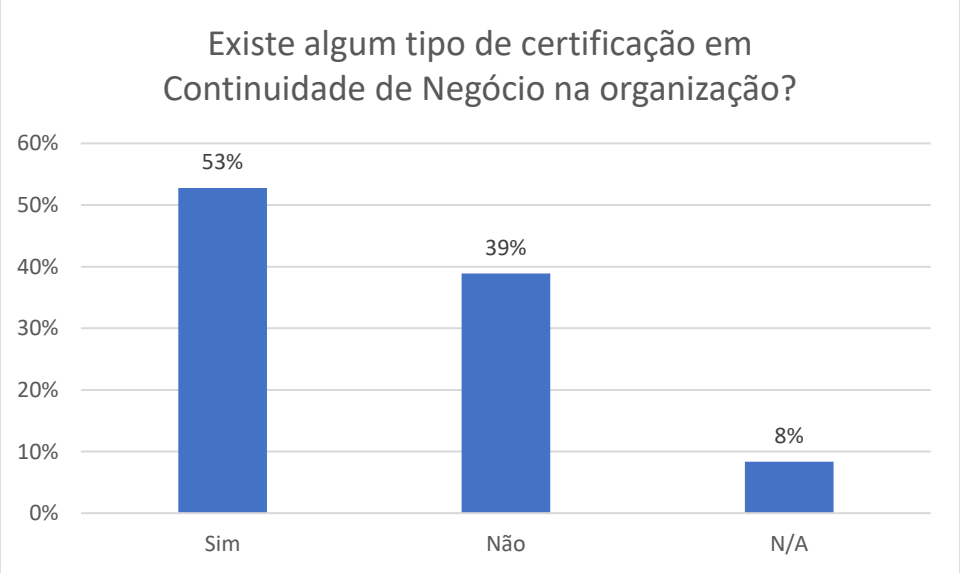

Figura 8.9 Existe algum tipo de certificação em Continuidade de Negócio na organização?

Fonte elaboração própria

Na questão em cima identifica procura-se identificar dentro da amostra obtida a existência ou não de certificações na área da continuidade de negócio.

Das 36 respostas obtidas o número mais expressivo (19) indica existir algum tipo de certificação nas organizações onde estão inseridos, 14 referem não existir qualquer tipo de certificação enquanto as restantes 3 respostas não foram conclusivas.

Das observações deixadas pelos inquiridos é possível ainda obter algumas informações adicionais sobre o tipo de certificações existentes e que vão de encontro ao que foi abordado ao longo do presente trabalho.

Entre as diversas observações deixadas 6 indicaram que a certificação está relacionada com a ISO 22301, 4 fizeram referência ao BCI e 1 ao DRI *International*, tendo todas estas sido abordadas ao longo do trabalho.

8.3.10 Questão 10. Estão identificados os ativos críticos para a organização?

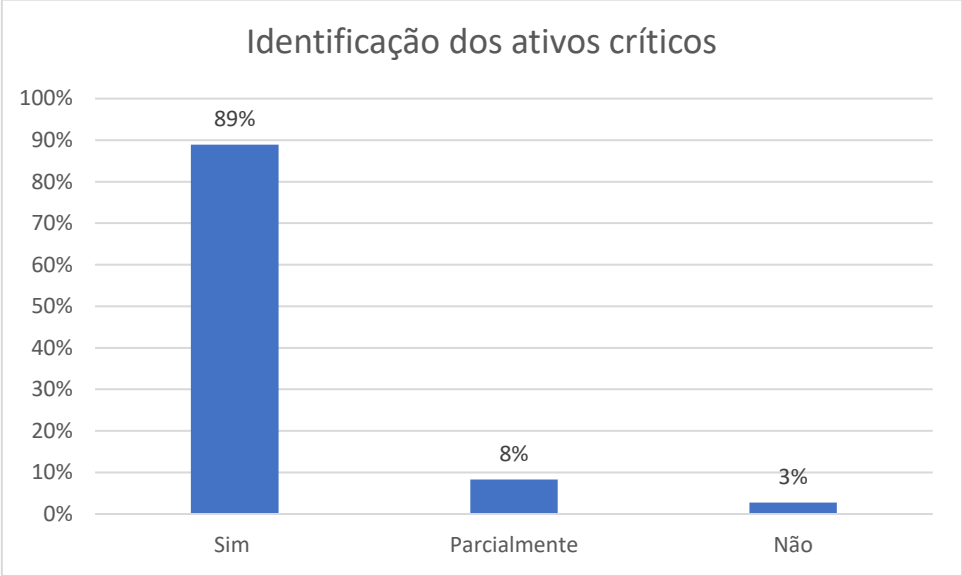

Figura 8.10 Identificação dos ativos críticos

Fonte elaboração própria

A identificação dos ativos críticos é uma das bases para a formação das políticas de continuidade de negócio, tendo a décima questão vindo reforçar esta ideia já referida ao longo do trabalho. Das 36 respostas obtidas apenas 1 indicou não terem os ativos críticos identificados e 3 indicaram que os ativos críticos estão apenas parcialmente identificados.

Dos comentários deixados nesta questão é de destacar um em que indica que face à observação de diversos clientes, os que tratam a continuidade de negócio como uma prioridade têm definidos os ativos críticos em diversos níveis incluindo ao nível dos processos.

Por outro lado, as organizações onde as políticas de continuidade de negócio não são da responsabilidade da gestão de topo acabam por definir estes ativos críticos apenas ao nível do IT e muitas vezes sem relacionar com processos.

8.3.11 Questão 11. Os critérios e metodologias aplicados nas Business Impact Analysis (BIA's) são aprovados pela administração/gestão de topo?

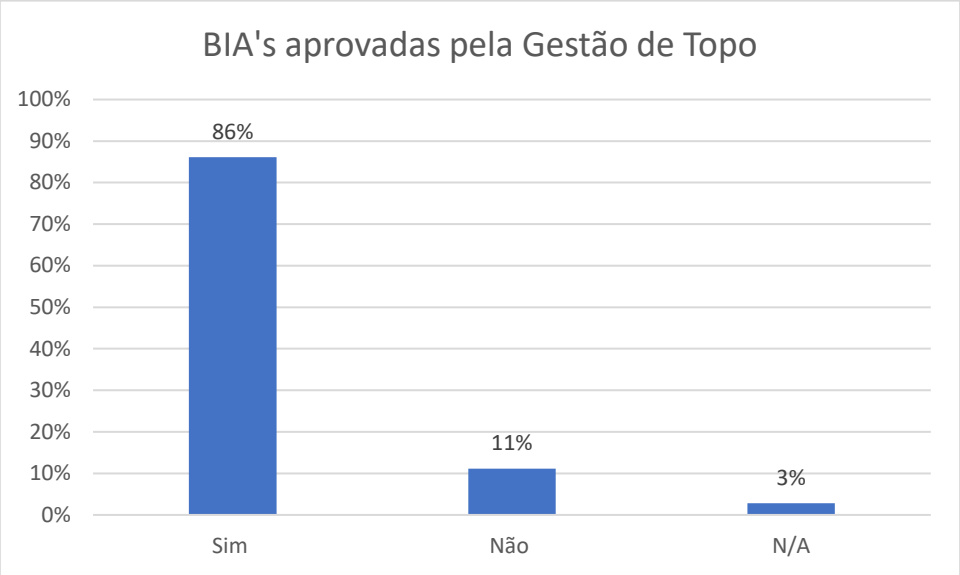

Figura 8.11 BIA's aprovadas pela Gestão de Topo

Fonte elaboração própria

A décima primeira questão, sobre a aprovação das BIA's por parte da administração, vem reforçar o que é referido no trabalho quanto à importância desta mesma aprovação. A grande maioria das organizações tem as BIA's aprovadas pela gestão de topo dentro da amostra obtida, sendo esta é a base para a formação dos PCN este é um ponto essencial para o sucesso destas políticas. Do total de 36 respostas 31 foram positivas, 4 negativas e 1 dada como "n/a".

Esta questão vem comprovar também a coerência das respostas ao longo do questionário uma vez que os resultados estão alinhados com a questão 8 sobre o envolvimento da gestão de topo na elaboração e testes aos PCN onde 5 dos inquiridos terão respondido negativamente à questão. Neste caso existe uma resposta que foi dada exatamente como "n/a", mas as 31 respostas positivas mantêm-se iguais nos dois casos.

8.3.12 Questão 12. O Plano de Continuidade de Negócio é parte fundamental do planeamento estratégico da organização?

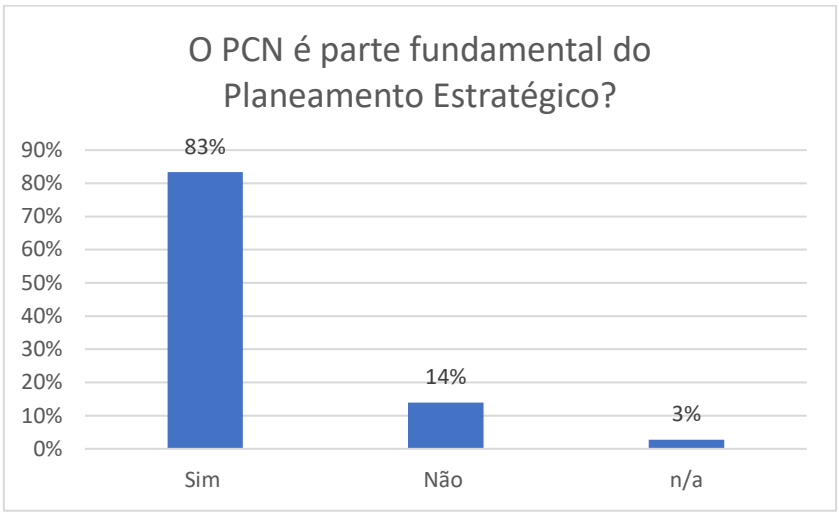

Figura 8.12 O PCN é parte fundamental do Planeamento Estratégico?

Fonte elaboração própria

A consideração das políticas de continuidade de negócio no planeamento estratégico das organizações é uma característica importante e que se pode verificar como presente na grande maioria das respostas obtidas, tendo 30 sido positivas, 5 negativas e 1 em que não foi possível tirar uma conclusão.

Não considerar na estratégia de uma organização a continuidade de negócio poderá levar a que as medidas implementadas não sejam transversais a toda a organização, e nem todos os processos críticos sejam tidos em consideração uma vez não estando ao nível estratégico estará focada por exemplo apenas num departamento por norma o de IT.

Num comentário deixado numa das respostas é feita a referência de que se tratando de uma entidade regulamentada no âmbito da continuidade de negócio os PCN são obrigatórios, e como tal têm de ser tidos em consideração no planeamento estratégico.

8.3.13 Questão 13. O Plano de Continuidade de Negócio inclui a existência de alternativas às infraestruturas da organização a nível físico, informático e de comunicações? (Ex: Hot site, Warm Site, Cold Site)

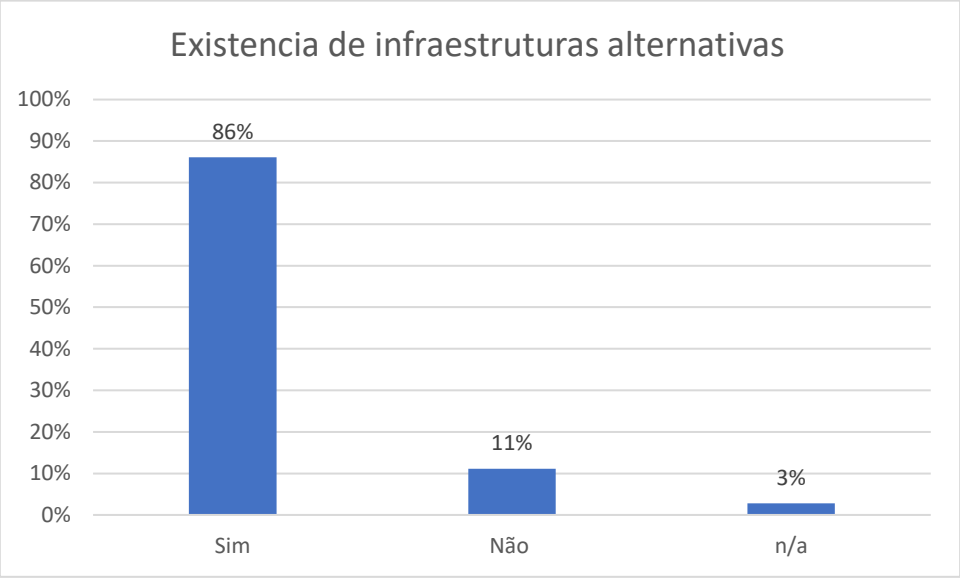

Figura 8.13 Existência de infraestruturas alternativas

Fonte elaboração própria

Quanto à existência de infraestruturas alternativas entre os 36 inquiridos a grande maioria (31) respondeu positivamente, confirmando a prática como comum entre as organizações com preocupações sobre continuidade de negócio e por isso algo recomendado conforme abordado no trabalho. Das restantes respostas 4 foram negativas e 1 classificada como "n/a" por não ser possível tirar uma conclusão.

Nas observações feitas a esta questão é deixado um alerta de algo que é observado com frequência pelo autor da resposta, que muitas vezes há organizações que têm apenas isto nos seus planos, ou seja, assumem que tendo infraestruturas alternativas nas mais diversas formas por si só é um PCN, o que obviamente não está certo.

Outra ideia importante deixada nas respostas a esta questão e que exemplifica que a continuidade de negócio não é um assunto linear para todas as organizações é a de um exemplo de uma empresa que após analisar as primeiras consequências da pandemia COVID-19 em 2020 concluiu que irá reestruturar os seus PCN.

Esta organização irá excluir os *hot sites* e *cold sites* existentes até ao momento mantendo apenas os existentes no estrangeiro. Este é um caso que é específico para a organização em questão e que não foi explicado em mais detalhe, mas que pode ser exemplificado por exemplo pelo sucesso da adaptação de todos os colaboradores em regime de teletrabalho, e por isso deixa de existir a necessidade de suportar infraestruturas alternativas para pessoal, passando a existir apenas a necessidade destas para os servidores da rede da empresa, podendo estar centralizadas noutro país.

Para o caso das organizações regulamentadas como é o caso da banca, foi deixado o comentário por um dos inquiridos que afirma que a existência de infraestruturas alternativas faz parte do processo de *compliance* junto dos reguladores como o banco central e agências de rating.

8.3.14 Questão 14. Existe um sistema específico para gestão de incidentes que define o papel de cada pessoa na organização e a sequência / linha de autoridade de cada um, em caso de ativação do Plano de Continuidade de Negócio?

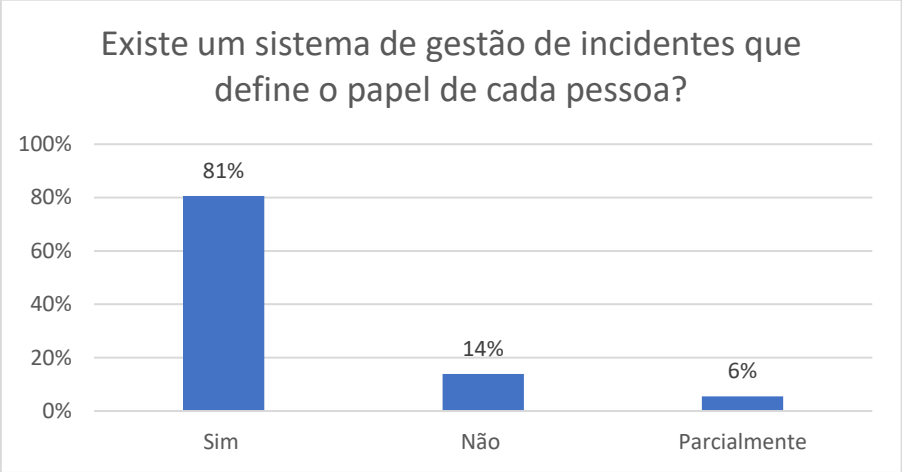

Figura 8.14 Existe um sistema de gestão de incidentes que define o papel de cada pessoa?

Fonte elaboração própria

Um aspeto fundamental para que as medidas e continuidade de negócio quando colocadas em prática funcionem com sucesso, é a existência de um sistema que define o papel de cada interveniente, bem como os diversos níveis de autoridade de cada um após ativação dos planos.

Do total de 36 respostas, 29 indicaram existir esta prática, enquanto 2 responderam que existia a pática apenas parcialmente, tendo as restantes 5 respondido negativamente à questão.

Nos mais diversos cenários o panorama da organização pode ser transformado de tal forma que os normais níveis hierárquicos dentro da organização podem não fazer sentido para determinadas situações, e as pessoas responsáveis por medidas como por exemplo a organização de todos os colegas para a mudança de local de trabalho e articulação com transportes serem por norma colaboradores que estão hierarquicamente a baixo daquelas que agora estão a coordenar.

A grande maioria dos inquiridos respondeu positivamente a esta questão, ajudando a comprovar que esta é uma prática comum e que deve ser aplicada pelas organizações que procuram ter políticas de continuidade de negócio que satisfaçam as suas necessidades.

8.3.15 Questão 15. A resposta aos incidentes está coordenada com entidades externas? (Ex: entidades publicas, autoridades, fornecedores, clientes, entre outros)

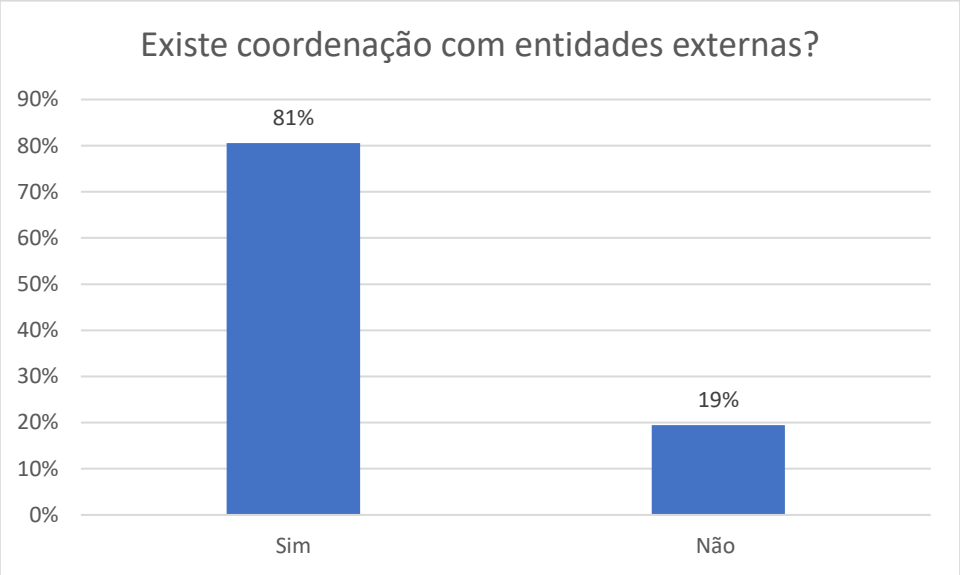

Figura 8.15 Existe coordenação com entidades externas?

Fonte elaboração própria

O planeamento da coordenação com entidades externas aquando da ativação dos PCN pode ser fundamental na hora em que as medidas forem colocadas em prática. A existência prévia de formas de comunicação ou até mesmo não existir necessidade de comunicação uma vez que os passos a seguir já estão coordenados com as diversas entidades externas, será uma mais valia para o sucesso das medidas de continuidade de negócio.

Neste sentido as respostas que na sua maioria confirmam a existência de medidas de coordenação com entidades externa, vieram ajudar na confirmação de esta como uma política utilizada com regularidade pelas organizações na amostra possível, tendo do total de 36 resposta apenas 7 indicado não ter esta prática.

Alguns comentários deixados pelos inquiridos ajudam a percecionar que tipo de coordenação externa existe nas organizações onde desempenham funções. É referida existência de coordenação com clientes, fornecedores, acionistas, entidades de supervisão e reguladores.

Alguns destes fazem sentido existir apenas em determinados setores, mas permite transpor para qualquer organização que a coordenação externa se pode estender a qualquer entidade com que exista alguma relação.

Além das já referidas, existe ainda uma observação deixada que indica além de clientes e fornecedores, existência de coordenação com forças de segurança, proteção civil e entidades governamentais aquando da realização de exercícios em determinadas instalações.

8.3.16 Questão 16. Estão implementados programas de treino / testes de modo a que os colaboradores respondam de forma calma e eficiente aos incidentes e com que frequência são feitos estes testes?

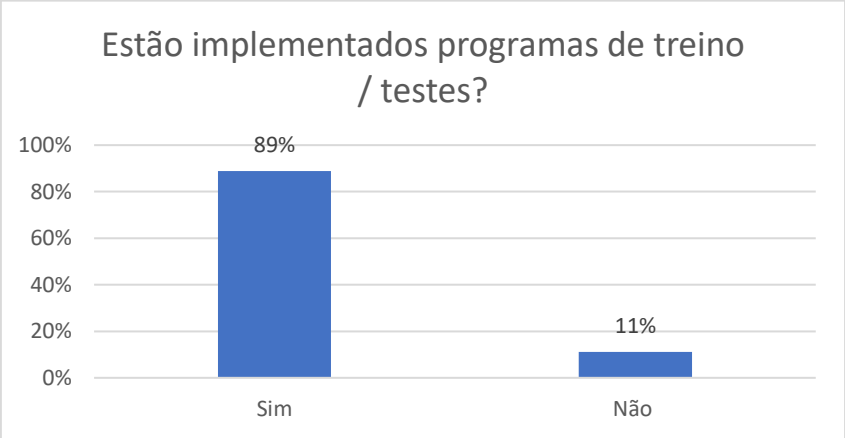

Figura 8.16 Estão implementados programas de treino / testes?

Fonte elaboração própria

A existência de programas de treino e realização de testes de forma a treinar os colaboradores para agirem da melhor forma em caso de ativação dos planos e ainda verificar a capacidades dos PCN cumprirem com os requisitos da organização é um dos pontos fundamentais da GCN abordado ao longo do presente trabalho.

As respostas à décima-sexta questão vêm confirmar a existência desta prática com bastante expressão dentro da amostra obtida, tendo 32 dos inquiridos respondido positivamente em relação à prática de testes enquanto apenas 4 deram uma resposta negativa.

Relativamente à segunda parte da questão que aborda a frequência dos testes, sendo o questionário de resposta aberta nem todos os inquiridos optaram por responder sobre este tema.

De entre os diversos comentários deixados sobre a frequência dos testes de salientar os mais comuns, como a realização de testes de uma forma anual, semestral ou trimestral.

Num dos comentários é feita a referência de testes realizados à totalidade dos procedimentos em ciclos de cinco anos, dando a entender que todos os procedimentos devem ser testados no mínimo a cada cinco anos. No entanto não fica claro se podem ou não existir procedimentos testados numa base mais regular ou se todos são testados apenas uma vez em cada cinco anos.

Apenas numa resposta é dada uma indicação da realização de testes apenas quando se entende necessário, não ficando por isso explicito quanto à frequência.

Uma solução apresentada numa das respostas é a realização de testes através de plataformas de *elearning* possibilitando assim a sua realização com maior frequência.

São ainda referidos dois casos em que os testes realizados são menos completos ficando apenas por testes de *Disaster Recovery* aos sistemas informáticos, não havendo assim abrangência de todos os procedimentos de continuidade de negócio.

No comentário considerado o que potencialmente poderá apresentar um sistema de testes mais completos é referido que estes são feitos duas vezes ao ano incluindo a total transferência das operações para o site de contingência e testes modulares para sistemas e operações específicas todas as vezes que existem alterações seja nos processos, seja nos sistemas que suportam os processos.

8.3.17 Questão 17. Existe dentro do Plano de Continuidade de Negócio, um plano de comunicação e gestão de crises? Quem é responsável pelo mesmo?

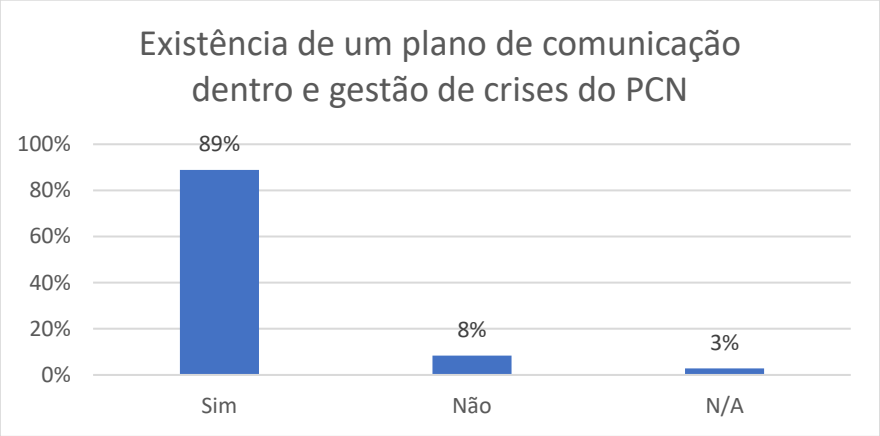

Figura 8.17 Existência de um plano de comunicação dentro e gestão de crises do PCN

Fonte elaboração própria

Na resposta à questão sobre a existência de um plano de comunicação e gestão de crises dentro do PCN já existente, é clara a confirmação de que esta prática é frequente na amostra obtida, tendo 32 dos 36 inquiridos respondido positivamente. Das restantes respostas 3 foram negativas e 1 dada como "n/a".

Através da análise dos comentários deixados nas respostas é possível obter informação adicional sobre quais as práticas habituais onde recai a responsabilidade pela comunicação nos planos. Tendo o questionário sido de resposta aberta nem todos os inquiridos forneceram em detalhe a resposta a esta última parte da questão.

Entre os comentários deixados, 8 (22% do total da amostra) indicaram que a responsabilidade fica a cargo das equipas de comunicação e gestão de crises, sendo que em alguns casos a comunicação fica a cargo do marketing que por norma pode já fazer trabalhos semelhantes.

Outra resposta que é dada também por vários inquiridos é a de que a responsabilidade pela comunicação é da administração, 5 dos inquiridos responderam neste sentido representando aproximadamente 14% do total da amostra.

Outras possibilidades apresentadas pelos inquiridos em respostas isoladas foram o IT Manager e RH Manager ou o departamento de risco como responsáveis pela comunicação aquando da ativação dos planos.

8.3.18 Questão 18. Considera que dada a importância de um bom Plano de Continuidade de Negócio, esta deve ser uma matéria auditada a nível interno e externo, sendo a auditoria um forte complemento aos processos de testes e melhoria contínua?

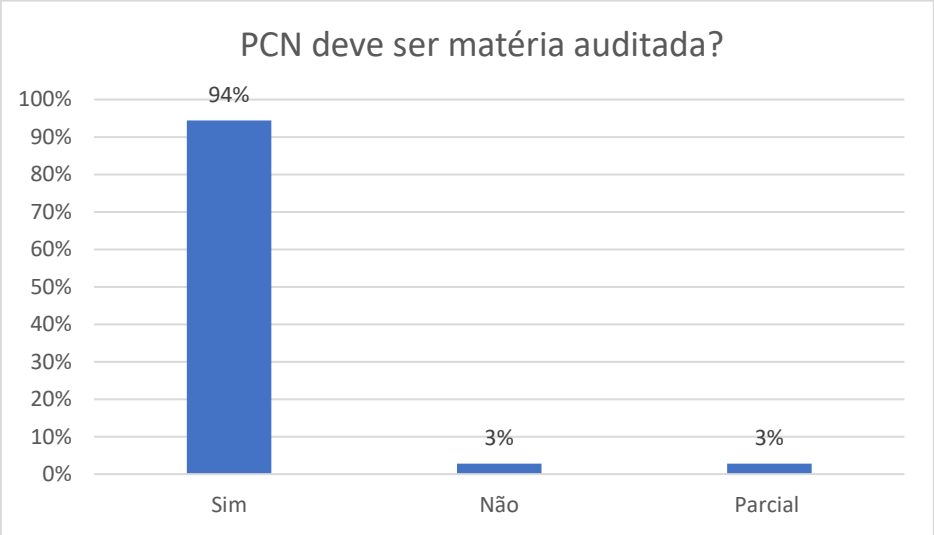

Figura 8.18 PCN deve ser matéria auditada?

Fonte elaboração própria

Na questão agora apresentada pretende-se apurar junto dos inquiridos se consideram importante a existência de auditorias aos PCN, sendo este um dos focos do trabalho, as respostas são claras tendo 34 dos 36 inquiridos respondido positivamente neste sentido.

Do total das respostas apenas 1 respondeu negativamente e outro respondeu que considerava que a nível interno deveriam sim existir auditorias, mas que tinha reservas quanto a auditorias externas, tendo por sido a resposta considerada como parcial para este efeito.

Das respostas dadas são de relevar alguns comentários deixados e considerados como um bom contributo para o presente trabalho.

Um dos inquiridos indicou considerar, além da importância das auditorias, que deveria existir um *benchmarkingh* e procura de partilha de boas práticas, tendo este sido um dos objetivos do trabalho onde são partilhadas várias fontes sobre as melhores práticas na área da continuidade de negócio.

Relativamente à auditoria é referido num dos comentários que estas complementam e podem detetar falhas nos planos, considerando, no entanto, mais importante a existência de testes.

A existência de auditoria aos PCN é considerada como determinante na melhoria contínua numa das respostas, que vai de encontro ao referido ao longo trabalho ao abordar este tema.

Para o caso das entidades sob a influência de regulamentos sobre continuidade de negócio, esta é uma questão que pode até nem fazer sentido uma vez que as auditorias a estas matérias fazem parte dos trabalhos habituais, o mesmo se aplica a organizações que optem por se certificar por exemplo na ISO 22301. Num dos comentários é ainda referido que existem organizações que recorrem a auditorias pois precisam de cumprir com determinados requisitos para prestar certos serviços.

Relativamente ainda a organizações que são regulamentadas nestas matérias, uma resposta dada por alguém que faz parte de uma instituição bancária refere que as auditorias são necessárias para manter o *budget* para a implementação e manutenção dos PCN, sendo um requisito do Banco Central a existência de auditorias internas e externas. Nesta resposta é referido ainda que considerar as auditorias um forte complemento pode ser exagerado, mas que sobretudo sem auditorias externas pode existir algum acomodamento, que consequentemente degrada os investimentos já feitos e o comprometimento com processos preventivos.

Um dos cometários deixados refere que as auditorias por representarem uma despesa são evitadas, e que apenas após ocorrerem incidentes se pondera as vantagens que estas poderiam ter trazido. Esta resposta foi considerada como positiva quanto à importância das auditorias, embora possa não ser claro, foi a interpretação feita, uma vez que dá a entender que após algo correr mal se coloca a possibilidade de recorrer a auditorias certamente com o intuito de procurar melhorias.

8.3.19 Questão 19. No seguimento dos recentes acontecimentos relacionados com o COVID-19 considera que o Plano de Continuidade de Negócio existente estava preparado para dar resposta, ou os acontecimentos foram tão imprevisíveis que foram tomadas medidas não planeadas, levando no futuro a uma revisão do plano existente?

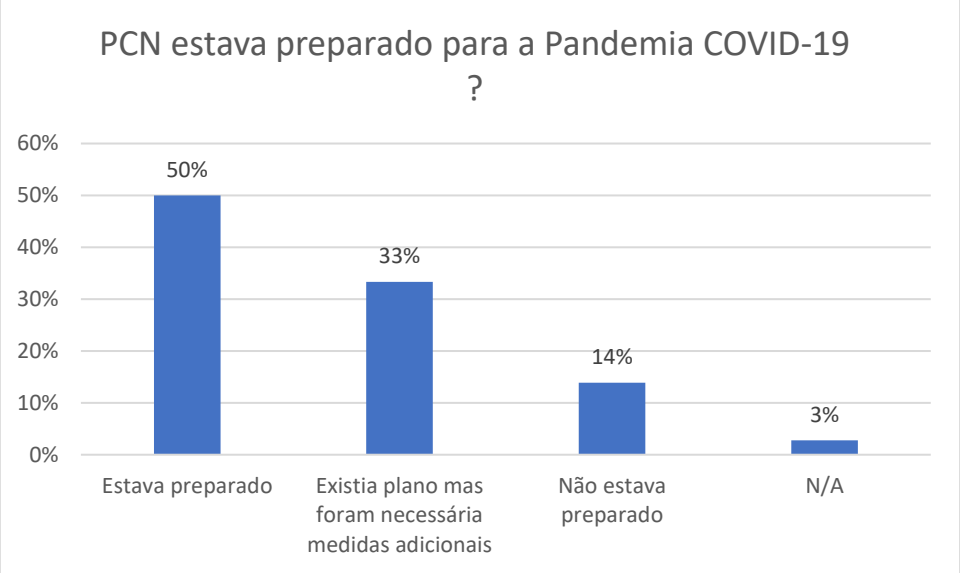

Figura 8.19 PCN estava preparado para a Pandemia COVID-19 ?

Fonte elaboração própria

No sentido de contextualizar o tema escolhido com a atualidade que se vive à data da elaboração do trabalho, a última questão aborda o tema da continuidade de negócio e a sua capacidade de responder aos eventos causados pela pandemia COVID-19 vivida no final de 2019 e pelo menos durante o ano de 2020 (data da elaboração do trabalho), não sendo a totalidade das consequências conhecidas ainda à data da realização do trabalho.

Do total dos inquiridos 18 respostas indicaram que os planos estavam preparados para a pandemia enquanto 12 das respostas deram a entender que embora tivessem planos foi necessário tomar medidas adicionais que não estavam previstas. Entre a totalidade das respostas 5 responderam ainda que os planos não estavam de todo preparados para os impactos da pandemia. Uma das respostas foi considerada como "N/A" uma vez que não foi possível interpretar a mesma em qualquer uma das hipóteses referidas anteriormente.

De relevar ainda são os diversos comentários deixados na questão com alguns relatos que podem servir de aprendizagem sobre o tema tratado no âmbito do presente trabalho.

Numa das respostas é referido que existia um plano pandémico revisto no início do ano de 2020 e que deu resposta até existirem casos confirmados positivos para o COVID-19 em Portugal.

A partir do momento em que surgiram os primeiros casos, dada a imprevisibilidade do tipo de vírus e as suas consequências, bem como as medidas tomadas pelos governos de diversos países foi necessário tomar algumas medidas adicionais não planeadas.

Quanto à importância dos PCN para as organizações, é possível verificar numa resposta dada que indica que no momento a principal preocupação de muitas empresas clientes é a sobrevivência face aos impactos da pandemia e que a revisão dos planos não está neste momento definida como uma prioridade, a menos que consigam perceber como os PCN as podem ajudar a sobreviver.

Embora acontecimentos como uma pandemia possam ser demasiado imprevisíveis nas suas variadas formas, a existência de planos que possam ser adaptados a diferentes casos pode ser certamente uma mais valia para a celeridade de resposta das organizações a eventos disruptivos.

É neste sentido que é deixado um comentário numa das respostas em que refere que embora os planos não estivessem preparados em particular para um evento como o COVID-19, os cenários já existentes permitiram uma mais rápida e eficiente gestão da disrupção.

Conforme é indicado em diversas respostas este tipo de acontecimentos disruptivos levam sempre a que as organizações retirem algumas aprendizagens e será certamente um motivo para procurar melhorar os planos existentes, sendo a melhoria continua um dos princípios básicos da GCN.

8.4 Análise dos resultados

De forma global quanto às práticas de continuidade de negócio referidas ao longo da presente dissertação e abordadas no questionário, a maioria dos inquiridos responderam positivamente quanto à aplicação das mesmas na realidade em que estão inseridos.

Com isto demonstra-se assim uma tendência, dentro da amostra obtida, que vai de encontro ao que são as recomendações referidas ao longo da investigação para as melhores práticas de continuidade de negócio nomeadamente:

- A administração/gestão de topo está altamente envolvida na elaboração e testes dos PCN (Questão 8);
- Existe algum tipo de certificação ao nível da Continuidade de Negócio (Questão 9);
- Estão identificados os ativos críticos para a organização (Questão 10);
- Os critérios e metodologias aplicados nas (BIA's) são aprovados pela administração/gestão de topo (Questão 11);
- O PCN é parte fundamental do planeamento estratégico da organização (Questão 12);
- O PCN inclui a existência de alternativas às infraestruturas da organização a nível físico, informático e de comunicações (Questão 13);
- Existência de um sistema específico para gestão de incidentes que define o papel de cada pessoa na organização (Questão 14);
- Coordenação com entidades externas (Questão 15);
- Estão implementados programas de treino / testes (Questão 16);
- Existência de um plano de comunicação e gestão de crises dentro do PCN (Questão 17);
- PCN deve ser uma matéria auditada a nível interno e externo (Questão 18).

À exceção da questão 9 em que 53% dos inquiridos responderam positivamente quanto à existência de algum tipo de certificação, em todas as outras questões em cima enumeradas mais de 80% dos inquiridos responderam de forma positiva quando às práticas abordadas nas questões sendo esta a tendência referida.

9 CONSIDERAÇÕES FINAIS

Ao longo da presente investigação foi feita a análise de algumas das principais fontes sobre o tema Continuidade de Negócio, com o objetivo de expor os principais conceitos existentes sobre o tema, dando assim ao leitor uma ampla perceção do que caracteriza um SGCN.

Sendo o assunto na realidade do tecido empresarial muitas vezes abordado apenas no âmbito dos SI, procurou-se demonstrar que o tema vai além disso e que a resiliência das organizações para ser robusta deve estar preparada para diversos tipos de cenários com impacto no normal desempenho das suas funções, que além dos SI devem abranger potenciais efeitos disruptivos de catástrofes naturais ou pandemias a título de exemplo. Os SI como componente fundamental da grande parte das organizações atualmente, também dependem de pessoas e infraestruturas que devem estar devidamente acauteladas nos planos.

Com o desenvolvimento e análise dos resultados da pesquisa efetuada, foi surgindo naturalmente a relação entre o tema continuidade de negócio com a auditoria interna, que desempenha uma função essencial de controlo interno, bem como a auditoria externa, que tem um papel fundamental nas organizações que procuram certificação nestas matérias.

No âmbito do tema da certificação foi possível apresentar algumas das principais possibilidades existentes para as organizações, sendo esta uma forma de atestar o mais alto nível de qualidade das políticas de continuidade de negócio quer a nível coletivo das organizações, quer a nível individual de profissionais especialistas nestas matérias.

De forma a ser possível constatar a realidade a nível nacional do que são as práticas de continuidade de negócio foram desenvolvidas duas entrevistas com profissionais responsáveis pelos PCN nas organizações onde desempenham funções, bem como a distribuição de um questionário online por profissionais com experiência ou a desempenhar funções relacionadas com o tema.

Através dos resultados obtidos quer das entrevistas quer do questionário, foi possível estabelecer uma relação entre os diversos assuntos abordados ao longo de toda a análise bibliográfica desenvolvida e aquilo que é aplicado ou recomendado como boas práticas pelos diversos inquiridos, dando assim um forte contributo para a qualidade do trabalho como um todo.

Desta forma foi possível reunir através da análise bibliográfica um vasto conjunto de boas práticas no âmbito da continuidade de negócio, que foram reforçadas pelos resultados obtidos nas entrevistas e questionários.

É de relevar como ponto forte do trabalho terem sido abordados temas no âmbito da continuidade de negócio relacionados com certificações que são dadas por organizações também elas fontes bibliográficas e que foram posteriormente referidas também pelos inquiridos, sendo assim possível fazer uma relação teórica do trabalho com a realidade empresarial.

Um aspeto positivo e considerado importante para o trabalho foi, dentro das respostas obtidas nos questionário e entrevistas, a função desempenhada pelos diversos inquiridos, que demonstra experiência nos assuntos abordados fazendo com que o seu contribuído traga alto valor acrescentado ao trabalho.

Algo menos positivo e considerado uma dificuldade para o trabalho foi a dimensão da amostra obtida, que embora satisfatória, sendo de uma dimensão maior, poderia representar de forma melhor a realidade empresarial como um todo. Esta dificuldade surge não por ser difícil encontrar organizações e profissionais com experiência nestas matérias, mas sim por considerarem este um tema sensível e que a exposição da realidade das suas práticas possa revelar algumas fragilidades ou até mesmo práticas que possam considerar que não devem ser tornadas públicas.

Outro aspeto menos positivo foi a dificuldade a nível nacional em encontrar centralizada uma fonte de informação sobre o tema continuidade de negócio, onde pudessem ser disponibilizadas algumas recomendações sobre as melhores práticas existentes. A existência da centralização deste tipo de matérias numa organização que tivesse um elevado estatuto de importância a nível nacional, seria uma mais valia na consciencialização da importância deste assunto, não só para a resiliência das organizações individualmente bem como para todo o mercado uma vez que a inexistência de boas práticas neste sentido pode representar elevadas perdas financeiras, falta de segurança para os trabalhadores ou até mesmo a perda de postos de trabalho.

Algumas recomendações para investigações futuras podem-se prender por exemplo com um maior detalhe de cada uma das práticas apresentadas de forma a disponibilizar para os leitores uma fonte de conhecimento sobre como as aplicar nas suas organizações.

Adicionalmente poderia ser desenvolvida uma investigação sobre que organizações poderiam desempenhar o papel de disponibilização de recomendações sobre continuidade de negócio para as organizações em geral a nível nacional, de forma a aumentar a consciencialização da importância deste tema.

Poderiam ainda ser encontradas soluções mais robustas para organizações de pequena dimensão que não tenham a possibilidade de fazer grandes investimentos neste sentido e que não sejam abrangidas por regulação especifica.

Poderá ainda ser valor acrescentado um estudo de mercado que permita compreender quantas organizações certificadas existem de facto em Portugal, bem como a interpretação que se pode fazer dos resultados obtidos relacionados com a dimensão das organizações.

Desta investigação poderão eventualmente surgir ideias de como se pode fomentar o crescimento destes números tornando o mercado como um todo mais resiliente face a eventos que provoquem interrupção das atividades.

Poderá a função de auditoria aumentar a consciencialização da importância deste tema em cada um dos seus clientes eventualmente disponibilizando mais serviços nesta área e contribuindo para o aumento da resiliência da sua carteira?

Nos setores não regulamentados deverá a auditoria interna e externa desempenhar a função de verificação da adequação das medidas de continuidade de negócio e desta forma conduzir as empresas a terem presente a importância da existência deste planeamento?

REFERÊNCIAS BIBLIOGRÁFICAS

AIG (Org.), *Cyber Edge,* disponível em, https://www.aig.com.pt/empresas/product/linhas-financeiras/cyberedge (Data da consulta: 14/06/2020)

BCI *CBCI Certification Course* disponível em, https://www.thebci.org/training-qualifications/business-continuity-certification-cbci.html (Data da consulta:18/06/2020)

BCI (Org.) *CBCI Certification Course* disponível em, https://www.thebci.org/training-qualifications/business-continuity-certification-cbci.html (Data da consulta:18/06/2020)

BCI & DRJ (2017) (Orgs.) *Glossary of Business Continuity Terms,* disponível em, https://www.thebci.org/asset/E6E7B9C3-355F-49D9-80340124B2E836E8

BCI Horizon Scan Report (2020) (Orgs.) *An examination of the risk landscape for resilience professionals,* disponível em, https://www.bsigroup.com/localfiles/en-gb/iso-22301/resources/bci-horizon-scan-report-2020.pdf

Bronack, T. (2012). *Auditing a BCP Plan,* disponível em, http://www.dcag.com/images/AUDITING_A_BCP_PLAN.pdf

Buehler K., Conjeaud O., Giudici V., Samandari H., Serino L., Vettori M., Webanck L., and White O. (2020) *Leadership in the time of the coronavirus: COVID-19 response and implications for banques (McKinsey & Company)* disponível em, https://www.mckinsey.com/industries/financial-services/our-insights/leadership-in-the-time-of-coronavirus-covid-19-response-and-implications-for-banks

CMVM, Banco de Portugal e ISP (atual ASF). (2010) (Orgs.) *Recomendações da sobre Gestão da Continuidade do Negócio*, disponível em, https://www.cmvm.pt/pt/Legislacao/Legislacaonacional/Recomendacoes/Documents/RecCNSFGCN.pdf

Disaster Recovery Institute International (DRII) *Center of Excellence in Resilience,* disponível em, https://drii.org/centerofexcellenceinresilience (Data da Consulta: 17/06/2020)

Disaster Recovery Institute International (DRII) *Certified Business Continuity Auditor (CBCA),* disponível em, https://drii.org/certification/cbca (Data da consulta: 17/06/2020)

Disaster Recovery Institute International (DRII). (2018) (Org.) *Glossary for Resilience,* disponível em, https://drii.org/glossarydocdowload/english/International_Glossary_for_Resilience_2018

Disaster Recovery Institute International (DRII). (2018) (Org) *The Professional Practices for Business Continuity Management,* disponível em, https://drii.org/resources/professionalpractices/EN

Federal Bureau of Investigation (FBI) (Org.) *The Morris Worm, 30 Years Since First Major Attack on the Internet*, disponível em, https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218, (Data da publicação, 02/11/2018)

Fidelidade (2020), *Multirriscos produtos negócios*, disponível em, https://www.fidelidade.pt/PT/empresas/Multirriscos/Produtos/negocio/Paginas/Negocio.aspx (Data da consulta: 12/06/2020)

ISO 22300 (2018) (Org) *Security and resilience – Vocabulary,* disponível em, https://www.iso.org/obp/ui/#iso:std:iso:22300:ed-2:v1:en

ISO 22301 (2019) (Org.) *Security and resilience — Business continuity management systems — Requirements*. International Organization for Standardization, disponível em, https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en

IT Gorvernance (Mar. 2019) (Org.) *Business Continuity and ISO 22301,* disponível em, https://www.itgovernance.co.uk/resources/green-papers/business-continuity-management-iso22301-faq

Jorrigala, V. D. (2018), *Business Continuity and Disaster Recovery Plan for Information Security*, disponível em, https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1068&context=msia_etds

KPMG (2006) (Org.) *Building a Continuity Culture,* disponível em, http://www.dcag.com/images/BusinessContinuity.pdf

KPMG (2016) (Org.) *Business Continuity Management,* disponível em, https://assets.kpmg/content/dam/kpmg/pdf/2016/06/hu-business-continuity-management.pdf

Manoel, S. S., (2019). *Sistema de Gestão de Continuidade de Negócios.* Rio de Janeiro: Brasport

Regulamento (UE) 2016/679 do parlamento europeu e do conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*

SANS Institute Information Security Reading Room (2006) *Business Continuity Planning Concept of Operations*, disponível em, https://www.sans.org/reading-room/whitepapers/recovery/business-continuity-planning-concept-operations-1653

Swanson, D. (2013) *How to Audit Business Continuity Programs*, disponível em, https://info.knowledge.com/bid/187874/how-to-audit-business-continuity-programs

Tranquilidade, *Outros Seguros*, disponível em, https://www.tranquilidade.pt/empresas/seguros/outras-ofertas/outros-seguros (Data da consulta: 12/06/2020)

ANEXOS

Anexo 1 Questionário distribuído online

Caracterização da Amostra

1. Qual a organização onde trabalha?
2. Qual o setor a entidade onde presta funções?
3. Qual o cargo que ocupa na organização?
4. Qual o número médio de trabalhadores?
5. Qual o ano de constituição da empresa?
6. A quem reporta na organização?

Questões

7. Qual o cargo desempenhado pela pessoa responsável pelo Plano de Continuidade de Negócio, e a que nível está na organização? (Ex. operacional, estratégico ou outro)
8. A administração/gestão está altamente envolvida na elaboração, e testes dos Planos de Continuidade de Negócio?
9. Existe algum tipo de certificação a nível da continuidade de negócio ou pessoas certificadas nestas matérias envolvidas?
10. Estão identificados os ativos críticos para a organização?
11. Os critérios e metodologias aplicados nas *Business Impact Analysis* (BIA's) são aprovados pela administração?
12. O Plano de Continuidade de Negócio é parte fundamental do planeamento estratégico da administração?
13. O Plano de Continuidade de Negócio inclui a existência de alternativas às infraestruturas da organização a nível físico, informático e de comunicações? (Ex: *Hot site, Warm Site, Cold Site*)
14. Existe um sistema específico para gestão de incidentes que define o papel de cada pessoa na organização, e a sequência / linha de autoridade de cada um em caso de ativação do Plano de Continuidade de Negócio?
15. A resposta aos incidentes está coordenada com entidades externas?
    (Ex: Entidades publicas, autoridades, fornecedores, clientes, etc.)
16. Estão implementados programas de treino/ testes de forma a que os colaboradores respondam de forma calma e eficiente aos incidentes, e com que frequência são feitos estes testes?
17. Existe dentro do Plano de Continuidade de Negócio um plano de comunicação e gestão de crises, e quem é responsável pelo mesmo?
18. Considera que dada a importância de um bom Plano de Continuidade de Negócio, esta deve ser uma matéria auditada a nível interno e externo, sendo a auditoria um forte complemento aos processos de testes e melhoria contínua?
19. Questão 19. No seguimento dos recentes acontecimentos relacionados com o COVID-19 considera que o Plano de Continuidade de Negócio existente estava preparado para dar resposta, ou os acontecimentos foram tão imprevisíveis que foram tomadas medidas não planeadas, levando no futuro a uma revisão do plano existente?

Anexo 2 Respostas ao questionário online na plataforma Survio

.

1 Qual é o tipo de organização (Pública, Privada, Terceiro Setor) onde trabalha?

Privada (24x)	Publica	Privada, consultoria de negócio e tecnologia	Privada - IT
privada (2x)	Privada.	segurança privada	Consultor de continuidade de negócio
Privado	Credito Agricola	IPSS	Empresa privada cujo único acionista é o estado

Escreve notas de rodapé para esse resultado

2 Qual é o setor de atividade da organização onde presta as atuais funções?

Serviços partilhados	Serviços (4x)	Transversal mas com maior enfoque no sector financeiro	Consultoria
Seguros não vida	Consultadoria (2x)	IT (2x)	Financeira (2x)
Industria	Serviços de Consultoria para clientes	consultoria em todos os setores	Telco
Sistemas de Informação	Retalho	Tecnologias de informação	Financeiro (3x)
Financeiro.	gestão	Banca - Gestão de Empresa	Consultoria informática
Serviços IT	Chefia	Managed Security Services	IT, Digital e Supply Chain
Comercial	Banca		Banco
Saúde e Serviço Social			

Escreve notas de rodapé para esse resultado

3 Qual é o cargo/posição que ocupa na organização?

Business continuity manager	Coordenadora de área	CISO	CEO (2x)
Associate Manager	Diretor (2x)	Gestor de Continuidade de Negócio	Diretor de Sistemas de Informação
Offering Manager	Técnico Sénior	Consultor Continuidade de Negócio	CEO e BC Consultant
CEO e consultor	Security Architect	Técnico	Diretor de negócio
Responsável pela Continuidade da Atividade	Responsável do Plano de Continuidade de Negócio	Business Manager	Consultor responsável de continuidade de negócio
Service Transition	Representante ao Cliente	ocupava, gestor de serviços	Diretoria
Comissão Executiva	Gerente	Gestor de Empresas	Gestor de Clientes
Comercial	Presidente do Conselho de Administração	Vice-presidente	Account Security Officer
Analista de segurança		Gestor de Continuidad de Negócio	

Escreve notas de rodapé para esse resultado

4 Qual é o número total de empregados?

550	12000	100	60
30	1500 (2x)	130	1000
cerca de 5000	350000	500	Modelo de colaboração com consultores externos quando necessário
500+	1	120	
30000	900	1200 em Portugal	45
75000	140 na minha area	54	Acima de 2000
Por volta de 600	450	7	4600 colaboradores
7200	800	16	6000
+20	130k	~ 10000	+1000

Escreve notas de rodapé para esse resultado

5 Em que ano a organização foi constituída?

2006 (2x)	1520	1960	2013
2008	1985 (2x)	1969	20
Há mais de 100 anos	1911	1990	2014 (2x)
2012 (2x)	1999	1792	1993
Já fez 100 anos	2011	1984 (2x)	2017 (2x)
1982	2015	2000	1991
1876 (2x)	1968	1964	muito antiga
1987			

Escreve notas de rodapé para esse resultado

6 A quem reporta na organização?

Operations manager	Diretor de área	Director	Administração
Socios	Administrador	CEO (4x)	Diretor do Departamento
Gestor de CN	GTS - Manager	CIO	Ao próprio
head of infrastructure	Diretor (2x)	Coordenador PCN	COO
Diretor de soluções tecnológicas	Field Services Manager	diretor nacional	Nada
Aos Sócios	Team Leader	General Manager / CRO	Diretor Comercial
Banco de Portugal	DIRECTOR DE AREA	Coordenador	ao diretor central
CISO	Presidente	Security Governance & Customer Compliance Manager	Diretor de IT

Escreve notas de rodapé para esse resultado

7 Qual é o cargo desempenhado pela pessoa responsável pelo Plano de Continuidade de Negócio e a que nível está na organização? (Estratégico, Tático ou Operacional)

A nivel internacional o cargo esta ao nível da administração do sector (a empresa esta dividida por global business units)	Estratégico (8x)	Administração, estratégico	Tático (3x)
CEO	Diretor de Sistemas de Informação, Nível Tático	Gestor de CN - Tático	Responsável pela área da qualidade
IT Business Manager, estratégico	Direção de Qualdiade	(nos meus clientes) (a minoria com cargo especifico a reportar à direção, mais comum responsável pela segurança acumula as funções de BCC, nas empresas mais pequenas o diretor de IT assume o DRP)	CIO
Táctico	Operacional (2x)		O cargo envolve todas as vertentes mencionadas, sendo maioritariamente estratégico e tático.
Estratégico/Operacional	N/A	Presidente da Comissão Executiva	Head of Risk - nível estratégico
Estrategico	diretor nacional	Presidente	Presidente do Conselho de Administração
Administrador, Estrategico	Manager Compliance (Responsável pelo Sistema de Gestão Integrado) / Nível Táctico		Direção Gestão de Risco, Estratégico

Escreve notas de rodapé para esse resultado

8 A administração/gestão de topo está altamente envolvida na elaboração e testes dos Planos de Continuidade de Negócio?

Sim (18x)	sim (3x)	SIM	é da responsabilidade da adm a elaboração, gestão e colocação em pratica do mesmo
Não (2x)	É o primeiro destinatário dos testes anuais de continuidade de negócio e participa em Table Top Exercices do Gabinete de Crise	(nos meus clientes) cada vez mais a empresas estão a percepcionar a importância dos BCP e por isso a administração de topo envolve-se e aumenta a prioridade do projeto	Sim por questões de compliance
Sim (ao nível da aprovação dos planos)	presumo que sim	Sim, diariamente envolvida	Suponho que sim
Não, o envolvimento é relativo ficando o mesmo pela aprovação dos planos elaborados	Sem duvida, numa grande organização de um Banco a administração está sempre interligado com todos os sectores de actividade		Comprometida, mas não envolvida diretamente. Tanto a elaboração como os testes são inteiramente realizados pela área de Risco
Não. A GT não revela grande interesse na Continuidade de Negócio apesar de indiretamente, nele gastar dinheiro de forma pouco alinhada com as necessidades.			

Escreve notas de rodapé para esse resultado

9 Existe algum tipo de certificação ao nível da Continuidade de Negócio e/ou pessoas envolvidas e certificadas nestas matérias?

Todos somos certificados mas nao temos nenhuma iso	Não (7x)	SIm, BCI e ISO22301	não
Sim, Iso 22301	Nao (3x)	Sim (7x)	Internamente,não, mas procuramos que os consultores externos sejam certificados
Existe a norma ISO 22301, embora em Portugal muito poucas empresas tenham esta certificação	Toda a equipa de CN está certificada na ISO 22301	sim (2x)	Sim ISO, DRII,BCI
Certificação ISO22301 Lead Implementer. Membro do BCI.	N/A	Não é exigida certificação externa mas existem formações específicas internas para as pessoas envolvidas na matéria.	não tenho conhecimento
	Sim, MBCI	Not Available	Sim, além do conhecimento académico é necessário experiencia
	NS		
	Não, nem creio que seja para breve algo do género. Apenas eu sou certificado ISO22301.		

Escreve notas de rodapé para esse resultado

10 Estão identificados os ativos críticos para a organização?

Sim (22x)	SIm	sim (4x)	Parcialmente
(nos meus clientes) Os que têm a liderança do BC no topo e/ou na segurança sim, os restantes têm apenas para o IT (soluções e aplicações) e muitas vezes sem relação com os processos de negócio	Sim existindo redundancia sempre que financeiramente possível	mal defenidos	Com certeza, isto é essencial e sem isto todo o plano se torna mera formalidade
	Sem, claramente.	Sim, estão completamente identificados os activos criticos.	Não
	Uma parte seim. As novas tecnologias não porque a empresa vê-as como pouco relacionada à Continuidade. A empresa tem tendência a confundir alta-disponibilidade com a não necessidade da Continuidade.		

Escreve notas de rodapé para esse resultado

11 Os critérios e metodologias aplicados nas Business Impact Analysis (BIA's) são aprovados pela administração/gestão de topo?

Sim (24x)	SIM	sim (3x)	Não (2x)
(nos meus clientes) Os que têm a liderança do BC no topo e/ou na segurança sim e inclusivamente estão alinhados com o gabinete de gestão de risco	N/A	nao tenho conhecimento	Tudo fica a cargo da área de risco representada pelo Head of Risk, não havendo uma aprovação formal, mas tudo é coordenado junto as demais diretorias
	Tudo num Banco é aprovado pela CECA.	O BIA é muito muito antigo e nessa altura foi aprovado pela Adm.	

Escreve notas de rodapé para esse resultado

12 O Plano de Continuidade de Negócio é parte fundamental do planeamento estratégico da organização?

Sim (20x)	Não (3x)	Quase, vai ser	sim (4x)
O plano de continuidade de negócio faz parte de obrigações regulamentares mais vastas e, como tal, tem que ser tido em conta no planeamento estratégico.	Sin	(nos meus clientes) Os que têm a liderança do BC no topo e/ou na segurança sim, porque é um requisito do grupo, ou acionistas ou do regulador	Nao
	não tenho conhecimento	Não. A empresa não tem planeamento estratégico no que à Continuidade de Negócio diz respeito.	O plano estratégico possui sessão dedicada ao plano de continuidade dos negócios
	Claramente que sim, todas as grandes organizações são obrigadas a ter um plano estrategico para melhor desempenhar as funções		

Escreve notas de rodapé para esse resultado

13 O Plano de Continuidade de Negócio inclui a existência de alternativas às infraestruturas da organização a nível físico, informático e de comunicações? (Ex: Hot site, Warm Site, Cold Site)

Incluiu até esta pandemia, as lições a tirar desta pandemia são muitas e vamos restruturar todo o plano, excluindo os hot e cold sites em Portugal mantendo apenas os no estrangeiro	Não (4x)	SIm, cold site	apenas a nível informatico
Sim, do ponto de vista digital a Banca desenvolveu muito nos ultimos 5 anos.	Sim (18x)	Sim, Cold Site.	sim (3x)
	(nos meus clientes) esta é a parte mais comum... a maioria das empresas só tem isto (muitas vezes confundem que isto é sinónimo de um BCP)	Alta disponibilidade	não tenho conhecimento
	Sim, desde 1992.	Em bancos isto faz parte do processo de compliance junto a reguladores como Banco Central e agências de Rating	Sim, temos estratégias e soluções implementadas para responder à indisponibilidade de Pessoas, Instalações, IT, OT e Supply Chain.

Escreve notas de rodapé para esse resultado

14 Existe um sistema específico para gestão de incidentes que define o papel de cada pessoa na organização e a sequência / linha de autoridade de cada um, em caso de ativação do Plano de Continuidade de Negócio?

Sim (23x)	Não (2x)	A parte operacional sim, falta o resto.	sim (3x)
(nos meus clientes) Os que têm a liderança do BC no topo e/ou na segurança sim, com ligação a segurança física e segurança de informação e privacidade de dados	nao	não, foi implemntado após surgirem situações que geraram mal estar interno	Não, é assegurado em comite de crise pelo CEO
	Sim e isto está refletido no BCP		Todas as funções dentro da organização Banca estão bem defenidas e deliniadas para cada função ou tarefa.
	Parcial. Ainda há muito trabalho a faezr nessa matéria.		

Escreve notas de rodapé para esse resultado

15 A resposta aos incidentes está coordenada com entidades externas? (Ex: entidades publicas, autoridades, fornecedores, clientes, entre outros)

- Estao incluidos e essa ponte é efectuada pelos responsáveis indicados no plano, exemplo formecedores de limpeza sao coordenados por facilities cujo manager faz parte da célula de crise
- não
- Algumas sim
- Não (4x)
- Fornecedores
- sim (2x)
- nao
- Sim, parcialmente
- Todos e sobretudo reguladores como o banco central
- Não. Um incidente que envolva entidades externas, será um verdadeiro desastre de RH e de consequências imprevisiveis para pessoas e bens.
- sim, estão incluidas no processo.
- Sim. O plano prevê comunicação com acionistas, clientes, fornecedores, entidades de supervisão e outras autoridades quando necessário.
- Está coordenada com os nossos clientes e principais fornecedores. Em algumas das nossas instalações, estamos alinhados e fazemos exercícios com as forças de segurança, protecção civil e entidades governamentais.
- clientes
- Sim (16x)
- (nos meus clientes) Os que têm a liderança do BC no topo e/ou na segurança sim, fazendo-o através dos planos de resposta a incidentes
- Sim está coordenada com entidades externas.

Escreve notas de rodapé para esse resultado

16 Estão implementados programas de treino / testes de modo a que os colaboradores respondam de forma calma e eficiente aos incidentes e com que frequência são feitos estes testes?

- Sim, teste geral anual e testes de "systems not available" tb anuais
- sim (2x)
- Sim (são feitos testes à totalidade dos procedimentos em ciclos de 5 anos)
- não
- Sim realizados através de plataformas de elearning com frequência.
- Alguns sim, mas não é sistemático
- Apenas testes de Disaster Recovery técnico. De Continuidade de Negócia "per si" não há.
- Não (3x)
- Trimestral
- (nos meus clientes) Os que têm a liderança do BC no topo e/ou na segurança sim, os restantes normalmente fazem apenas uns testes ao nível de informática (interno ao departamento de IT) e sem colaboração dos outros colaboradores
- Sim, embora apenas vise as equipas envolvidas no PCN). Testes feitos anualmente.
- Sim (13x)
- Sim, no mínimo um teste anual.
- sim, anual
- Sim anualmente ou sempre que faça sentido
- Sim. Formalmente, a cada 6 meses, mas, fruto da estratégia escolhida, acabamos por testar as soluções com mais frequência,
- Sim, testes semestrais (TI) e anuais (Evacuação)
- os testes são realizados anualmente
- Os testes são realizados de forma adhoc
- Sim , com a frequência determinada pelas políticas do grupo.
- Sim e são feitos duas vezes ao ano testes completos (total transferência das operações para o site de contingência e testes modulares para sistemas e operações específicas todas as vezes que existe alterações seja nos processos, seja nos sistemas que suportam os processos.

Escreve notas de rodapé para esse resultado

17 Existe dentro do Plano de Continuidade de Negócio, um plano de comunicação e gestão de crises? Quem é responsável pelo mesmo?

Existe, os responsáveis são a equipa global de comunicação e a célula de crise	Não (2x)	SIm, gabinete de comunicação	Marketing
sim CEO	Gerente de mudanças	Sim. Todos os planos são coordenados pela gabinete de crise e executados pelos departamentos responsáveis (p.e., Comunicação - Departamento de Marketing)	A administração
Sim (5x)	Gabinete de comunicação	São temas separados mas complementares.	Existe um PCN que contempla vários planos
Sim. O DPO	(nos meus clientes) Os que têm a liderança do BC no topo e/ou na segurança sim, como parte do plano de gestão de crise e adaptado para vários tipos de cenários	Sim, IT Business Manager e RH Manager	sim, cio
Sim (Head of Media Relations)	N/A	Tudo fica a cargo da área de Risco	Comissão de Gestão de Crises (composta por membros da Administração e órgãos de recursos humanos, comunicação, sistemas e tecnologias, gestão de riscos, auditoria e operaçoes)
Sim, responsável de comunicação e administração	não, o diretor nacional	Sim. Gestão de topo	Temos um documento único que inclui todas as disciplinas indicadas acima. O Plano está sob a minha responsabilidade enquanto membro da CE. Adicionalmente, última responsabilidade é do Presidente do Conselho de Administração.
Sim, administração	Sim existe e é sempre nomeado pela CECA.	Administrador	
Sim. Existe uma equipa responsável, desconhecendo quem são os elementos.	Caixa Central de Credito Agricola	Nim. Existe mas na área de Incidentes não gerida pela área de Continuidade.	
Direção de Comunicação e Marca			

18 Considera que dada a importância de um bom Plano de Continuidade de Negócio, esta deve ser uma matéria auditada a nível interno e externo, sendo a auditoria um forte complemento aos processos de testes e melhoria contínua?

Considero que deve ser auditada e ser feito benchmarking e procura de partilha de boas práticas	Sim (20x)	Sim. Complementam e podem detetar falhas no plano (o melhor são so exercicios)	a nivel interno sim, quanto a auditorias externas tenho as minhas reservas.
Sim, já o é.	Sim, a auditoria tem um papel determinante na melhoria contínua	sim (2x)	(nos meus clientes) normalmente só nos que pretendem alcançar a certificação ISO 22301(porque isso lhes trás uma vantagem competitiva) e/ou têm que responder a requisitos para poder prestar serviços em clientes
As auditorias são necessárias para manter o budget para a implementação e manutenção dos planos de continuidade. Em bancos isto faz parte dos requisitos do banco central , tanto internamente como externamente. Quanto a um forte complemento, seria um exagero dizer “forte” , porém sem as auditorias, sobretudo externas, existe um ‘acomodamento” que degrada investimentos e o comprometimento com os processos preventivos.	Obviamente que sim e essa situação está normalmente regulada	auditorias custam dinheiro e norma geral este tipode situação é idada internamente de modo a evitar a despesa, caso ocorra um incidente depois logo se pensa nos custos que se poderiam ter evitado	Absolutamente. Mas ou se audita com seriedade, ou de nada serve auditar!
	Sim. (2x)		
	Correcto, somos frequentemente auditados.		
	Nao		

Escreve notas de rodapé para esse resultado

19 No seguimento dos recentes acontecimentos relacionados com o COVID-19 considera que o Plano de Continuidade de Negócio existente estava preparado para dar resposta, ou os acontecimentos foram tão imprevisíveis que foram tomadas medidas não planeadas, levando no futuro a uma revisão do plano existente?

Existia um plano pandemico, foi revisto em Janeiro e deu resposta enquanto o surto nao chegou a Portugal. Após isso tivemos de introduzir soluções não planeadas. Esta situação deveu-se a imprévisibilidade do virus em si, e das medidas que os governos foram tomando. Seja como for antes da declaração do estado de emergência tinhamos o escritório fechado	O plano não estava preparado para os acontecimentos.		O Plano existia e mas teve que ser ajustado à nova realidade
Apesar do PCN incluir uma estratégia robusta e operacional. Existiram acontecimentos improváveis. No futuro o PCN terá que ser revisto.	estava preparado	Sim (8x)	Não
O plano estava preparado para dar resposta a este tipo de acontecimentos.	O plano terá de ser revisto e atualizado	O plano está preparado para dar resposta a cenários não planeados. No entanto, em futuras revisões será equacionada a criação de cenários de epidemia / pandemia.	sim
	sim, estava preparado		De acordo com o resultado de questionários que executei, as empresas que tinham planos pandémicos utilizaram-nos (embora não estivessem preparados para esta situação), as restantes improvisaram. Quanto ao futuro, temos um número elevado de empresas cuja sobrevivência é ainda incerta pelo que, a revisão dos planos não estará nas suas prioridades a menos que as empresas consigam perceber o como o BCP as pode ajudar a sobreviver.
	Sim, a maior parte do trabalho pode ser efetuado em teletrabalho com as ferramentas existentes como skype e zoom. As auditorias e consultoria e formação apenas têm sido adiadas por falta de condições dos clientes	O plano é funcional e sem necessidade de revisão	
	A particularidade do cenário em causa não estava previsto no plano, mas os cenários acordados no plano permitiram uma mais rápida e eficiente gestão da disrupção.	Foram tomadas medidas não planeadas devido à expecificidade do tema. No fututo, alguns melhoramentos serão feitos ao Plano.	
		Sim estava	
		espero que sim	
O PCN existente estava apenas parcialmente preparado. Não só pela imprevisibilidade, mas também pelos contornos dos acontecimentos e suas repercussões, foram tomadas medidas não contempladas no plano existente, que possivelmente serão consideradas numa futura revisão.	Acredito que niinguêm estava preparado para uma pandemia, mas tivemos todos que nos reenventar, trabalhar mais e mais para que todos juntos possamos minimizar o impacto da COVID-19.	Sim, activámos o plano e não tivemos qualquer quebra de serviço, apesar do plano estar sempre a ser alvo de melhoria contínua.	No caso especifico já existiam um plano de continuidade inteiramente definido anteriormente por conta do Ebola, contudo este plano caiu em descrédito e foi taxado de exagerado onde muitos recursos requisitado como dispensadores de álcool gel foram cortados.
	O plano existente não se adequava ao Covid	Estava preparado	
Não estava preparado, mas acabou por se razoávelmente suave a implementação porque apenas passou por colocar as pessoas a trabalhar em casa controlada e atempadamente. Um desastre com indisponibilidade de recursos, garantidamente não terá o mesmo desfecho.	O PCN estava adequado, mas as infraestruturas existentes foram insuficientes para as necessidades	Todos os planos são dinamicos pelo existem sempre melhororias a efectuar, independemente do planeado	Não estava adaptado. Foi contudo das primeiras IPSS a ter um plano de contingência aprovado pela Segurança Social.

Anexo 3 Questões abordadas nas entrevistas

Caracterização da Amostra

1. Qual a organização onde trabalha?
2. Qual o setor a entidade onde presta funções?
3. Qual o cargo que ocupa na organização?
4. Qual o número médio de trabalhadores?
5. Qual o ano de constituição da empresa?
6. A quem reporta na organização?

Questões principais

1. Deve existir uma separação clara entre Continuidade de Negócio e Recuperação de Desastre?
2. As pessoas responsáveis pelos planos de Continuidade de Negócio devem ser parte das equipas de IT?
3. A administração/gestão deve estar altamente envolvida na elaboração, e testes dos PCN?
4. O foco dos PCN deve incidir noutras áreas além dos Sistemas de Informação? (mobilidade dos colaboradores/ infraestruturas alternativas/logística entre outros)
5. Os sistemas de *Backup* devem estar disponibilizados em mais do que um local?
6. A certificação ISO:22301 deve ser uma preocupação?
7. Devem estar pessoas certificadas nestas matérias, por entidades externas, envolvidas nos processos? Exemplos de entidades que dão certificações são:
    - Disaster Recovery Insitute;
    - Business Continuity Institute;
    - Certified Information Security;
    - Mile2;
    - EC-Council;
8. Deve estar clara no PCN a coordenação entre as equipas de IT e de Logistica/ *Facilities Management?*
9. O departamento de Planos de Continuidade de Negócio deve estar inserido no departamento de Gestão de Riscos / Segurança?
10. Devem estar contempladas no PCN medidas alternativas para o caso de falhas dos principais fornecedores?
11. Deve existir uma hierarquização dos principais fornecedores por grau de importância para a organização?
12. Devem estar contempladas no PCN medidas para fazer face a eventos disruptivos relacionados com questões legais? (pequenas alterações na lei que possam provocar grandes mudanças no modelo de negócio)
13. O PCN deve ser parte fundamental do planeamento estratégico da administração / gestão?
14. A gestão de risco, continuidade de negócio e segurança poderão ser tratados em conjunto num programa de resiliência da entidade?
15. Com que regularidade devem ser efetuados testes?
16. O PCN deve ser apresentado e estar disponível transversalmente a toda a organização como sendo uma necessidade fundamental do negócio?
17. Deve existir uma *framework* interna para o plano de continuidade de negócio?
18. Devem estar enumerados os riscos potenciais?
19. O PCN deve contemplar medidas que visam minimizar a probabilidade de ocorrência desses riscos?

20. Deve estar contemplado no PNC, uma ordem sequencial de prioridade, por importância, das funções a serem repostas em casos de ativação do PCN?
21. Deve existir um sistema específico para gestão de incidentes que define o papel de cada pessoa na organização, e a sequência / linha de autoridade de cada um?
22. A resposta aos incidentes deve estar coordenada com entidades externas?
    (Ex: Entidades publicas, autoridades, fornecedores, clientes, etc.)
23. Devem ser implementados programas de treino/ testes de forma a que os colaboradores respondam de forma calma e eficiente aos incidentes?
24. As medidas devem estar prontas a executar em qualquer momento?
25. Devem estar contempladas no PCN medidas para que sejam estabelecidas as comunicações necessárias a nível interno e externo de forma eficaz por toda a organização?

Anexo 4 Bruno, D., Costa M., and Rodrigues, F. (2021). Auditoria a Planos de Continuidade de Negócio. *In*: Bastos, M. A., Marques, R. P., Peguinho, C., and Caçador, S. (eds.). *Proceedings of the 1st International Conference in Accounting and Finance Innovation: business innovation and digital transformation, Universidade de Aveiro, Portugal, November 12-13, 2020. pp. 83-93.*

ISBN é 978-972-789-665-3.

Doi: 10.34624/1r78-9p55

"Auditoria a Planos de Continuidade de Negócio"

Abstract

A complexidade e a dimensão das organizações obrigam a que, cada vez mais, as administrações e a gestão de topo se preocupem em demonstrar um nível da maturidade e resiliência elevados perante o mercado. Este alto nível de maturidade pode ser observado na qualidade e eficácia dos seus produtos ou serviços, mas também no desempenho financeiro, impacto social, ambiental, entre outros.

Um aspeto que demonstra um elevado nível de maturidade de uma organização é a capacidade que esta tem de subsistir e continuar as suas operações em momentos de maior dificuldade, sejam por razões naturais de mercado ou em situações de desastre, sejam estas causas naturais ou provocadas por ataques de terceiros.
A gestão na continuidade de negócio preocupa-se em desenvolver planos suficientemente abrangentes, que preparem as organizações para continuar as suas operações em caso de ocorrência de eventos disruptivos, em diversos cenários possíveis. Estes eventos que causam interrupção das operações, mais habitualmente observados nos sistemas de informação, podem também ocorrer com consequências físicas, seja por desastres naturais ou pandemias.

No âmbito da gestão de risco importa para as organizações ter Planos de Continuidade de Negócio que visem atestar a resiliência das empresas e a capacidade que estas têm de continuar a prestar os seus serviços durante e após eventos disruptivos.

Sendo este um tema de elevada importância e que prepara as organizações para a mitigação de diversos riscos, importa atestar a qualidade e eficácia destes planos através de certificações e auditorias independentes.
O presente artigo procura dar uma resposta e identificar aquilo que são as principais características que os Planos de Continuidade Negócio devem incluir nas organizações. Foi realizada uma análise bibliográfica de fontes relevantes quer sobre regulamentação, quer sobre orientações a nível internacional.

A presente contribuição sugere identificar os pontos essenciais sobre os quais as auditorias devem incidir, de forma a documentar a conformidade dos resultados com o planeamento feito inicialmente.

Keywords

"Auditoria; Planos de Continuidade de Negócio; Sistemas de Informação; Resiliencia; Gestão de Risco"

Introdução

Dado o avanço tecnológico que enfrentamos, a forte dependência dos Sistemas de Informação (SI) é cada vez mais um fator que influencia as decisões das organizações. Esta dependência implica que estes sistemas sejam vistos como essenciais para o normal desempenho das funções da organização e as suas eventuais falhas, como situações críticas para a continuidade do negócio. Para garantir a resiliência da organização como um todo, em conformidade com o planeamento de gestão de risco, importa que existam medidas bem definidas e testadas, que visem a recuperação do negócio em caso de desastre e não menos importante, a continuidade das operações vitais com as condições mínimas, nos momentos imediatos após e durante os eventos disruptivos, quer estes sejam de natureza tecnológica ou física.

A elaboração e manutenção de Planos de Continuidade de Negócio (PCN) e Planos de Recuperação de Negócio (PRD), podem ser fatores decisivos para garantir a continuidade das organizações em caso de ocorrência de eventos disruptivos que afetem negativamente o normal desempenho das funções básicas das organizações em questão. Empresas que não demonstrem este tipo de maturidade e que não tenham planos preparados com medidas que visem mitigar os impactos negativos de eventos disruptivos para os mais diversos cenários possíveis, podem correr o risco de o tempo de resposta aos impactos negativos destes eventos ser demasiado longo e dispendioso pondo em causa a continuidade de determinados negócios ou mesmo da organização como um tudo.

Como noutros tipos de sistemas normalmente implementados nas organizações, a função de Auditoria desempenha um importante papel de garantia e controlo da conformidade dos planos com a sua aplicação prática. Importa ainda existir a verificação de planos de manutenção e melhoria contínua, sendo a função de Auditoria a que tem a responsabilidade de fazer uma análise independente e objetiva fornecendo um parecer imparcial sobre a qualidade dos planos em questão.

Pretende-se por isso com o presente trabalho fazer uma breve introdução ao tema da continuidade de negócio abordando alguns conceitos básicos, bem como estabelecer a relação com a função de Auditoria, através de uma revisão bibliográfica e um trabalho empírico que suporte a parte teórica do trabalho com a realidade destes assuntos em organizações reais.

Metodologia

Foi recolhida e analisada bibliografia, bem como, documentação emitida pelas organizações que regulam e emitem recomendações sobre estas temáticas a nível internacional. A análise bibliográfica efetuada pretende apresentar os principais conceitos sobre o tema escolhido e demonstrar a importância do mesmo estabelecendo, a relação com a função de Auditoria que é um objetivo do presente trabalho.

Foi ainda feita a leitura de publicações por parte de entidades públicas bem como empresas especializadas em auditoria e desenvolvimento deste tipo de planos de forma a adicionar à pesquisa efetuada o entendimento de organizações cujo seu contributo é de elevado valor acrescentado.

Foram ainda feitos levantamentos junto de organizações a nível nacional sobre como se aplicam estas orientações, tendo sido recolhida informação sobre alguns pontos essenciais de forma a estabelecer uma relação entre os assuntos teóricos e a realidade empresarial.

Revisão da Literatura

Plano de Continuidade de Negócio (PCN) – Definição

Em 2018 o *Disaster Recovery Institute* (doravante designado por DRI) no seu glossário para a resiliência, define um Plano de Continuidade de Negócio (PCN), como um conjunto de procedimentos e informações, devidamente documentados e desenvolvidos, que estão prontos para ser postos em execução a qualquer momento em caso de ocorrência de um evento disruptivo. Estes procedimentos permitem que uma organização possa dar continuidade aos seus produtos e serviços a um nível aceitável após o incidente se verificar, situação que é inicialmente definida em termos de planeamento.

Neste mesmo glossário publicado pelo DRI, um evento disruptivo é definido como um acontecimento que de alguma forma interrompe as operações ou processos da organização. Estes acontecimentos podem ser previsíveis ou antecipados como é o caso de tempestades ou crises políticas, ou podem-se tratar de eventos que não podem ser antecipados como um *Blackout,* ataque terrorista ou falha tecnológica.

De acordo com o *IT Governance* (2019) a continuidade de negócio é uma disciplina que se foca primariamente em preservar a capacidade que uma organização tem em funcionar durante um evento disruptivo, assegurando que as suas funções mais críticas continuam, mesmo que com uma capacidade mais reduzida.

A KPMG em 2006 referia que a disciplina de PCN ajuda as organizações na gestão de risco para os sistemas críticos, como o caso das redes partilhadas de informação e comunicação, contra eventos de causas naturais, eventos com intervenção humana ou mesmo motivos políticos, que de alguma forma ponham em causa a capacidade de continuar o negócio dentro da normalidade.

Em 2016, a KPMG redefiniu na sua abordagem de negócio um PCN em sete pontos essenciais que cobrem todo o ciclo de vida da gestão de continuidade de negócio, sendo eles os seguintes:

- Análise de impacto no negócio;
- Avaliação de ameaças e vulnerabilidades;
- Definição dos ativos críticos para o negócio;
- Definição da estratégia de continuidade de negócio;
- Preparação do PCN e Plano de Recuperação de Desastres (PRD);
- Testes e formações;
- Manutenção.

De acordo com Jorrigala (2018) um PCN de negócio é composto por:

- Gestão do próprio PCN;
- Análises de Impacto no Negócio ou *Business Impact Analysis* (BIA's);
- Planeamento das medidas para colocar em prática o PCN;
- Dependência do estado de prontidão do PCN;
- Testes, manutenção, e auditoria ao PCN.

Objetivos

De acordo com Bronack (2012), um bom PCN deve conter nos seus objetivos:

- Proteção dos colaboradores;
- Recuperação de processos ou funções críticas para o negócio de forma a minimizar o impacto do desastre;
- Recuperação de infraestruturas e sistemas de suporte às funções consideradas críticas;
- Prevenção e mitigação dos efeitos de um desastre possível de ocorrer a qualquer momento;
- Proteção dos ativos da organização;
- Minimização dos impactos negativos do ponto de vista legal.

Responsabilidade sobre os PCN

Num questionário realizado a decisores de empresas canadianas publicado pela KPMG (2006), é referido que o desenvolvimento de um PCN deve envolver, não só os principais fornecedores de SI, mas também todas as áreas que utilizam esses mesmos sistemas e a administração. O envolvimento de toda a organização é fundamental pois de um ponto de vista dos processos que são muitas vezes transversais a várias áreas das organizações, devem haver planos que possam garantir a continuidade dos mesmos em caso de desastre e por isso não se podem focar apenas numa determinada área não abrangendo os processos do inicio ao fim.

A cultura de continuidade deve ser transversal a toda a organização e transmitida de uma forma vertical começando pela administração. Devem estar devidamente definidas responsabilidades e reportes em caso de ativação dos PCN de forma a tudo ocorra com o mínimo de perturbações possíveis.

Uma das principais dificuldades será a de manter a gestão consciente da importância de considerar os PCN no planeamento estratégico, operacional e orçamental das atividades que suportam o negócio. Para isto é importante que os planos estejam devidamente definidos nas organizações como fundamentais, servindo de proteção para as pessoas, prevenção contra perdas financeiras e garantia de maior confiança por parte do mercado.

Análise de Impacto no Negócio

As análises de impacto de negócio ou *Business Impact Analysis* doravante BIA's de acordo com o vocabulário da norma internacional ISO 22300 sobre segurança e resiliência, são definidas como a análise das atividades e processos, e quais os efeitos que os eventos diruptivos destes, podem trazer ao negócio.

De uma forma mais simples, mas cujo conceito se aproxima ao apresentado anteriormente, o DRI (2018) no seu glossário define as BIA como *"[a] method of identifying the effects of failing to perform a function or requirement."*

Em 2016 a KPMG definiu as BIA's como o processo que identifica e ordena por importância, as atividades e os ativos críticos para o negócio, bem como, o tempo máximo aceitável que estes podem estar em baixo e levam a ser reativados.

De acordo com o DRI (2018) no guia das práticas profissionais os objetivos das BIA's passam por:

- Identificar e ordenar por prioridade, as funções e processos de forma a definir quais terão maior impacto na organização em caso de falha;
- Avaliar quais os recursos necessários para suportar os processos de análise de impacto no negócio;
- Analisar os resultados obtidos e identificar eventuais diferenças entre os requisitos da organização e a sua capacidade de cumprir com esses requisitos.

Para que as BIA's possam ser efetivamente de utilidade, é importante que sejam respondidas algumas questões que Bronack (2012) define como:

- As BIA's desenvolvidas estão documentadas e alinhadas com os critérios definidos?
- Está estabelecida uma metodologia para desenvolver as BIA's e documentar os resultados?
- As BIA's finais foram aprovadas pela administração?
- As estratégias da recuperação estão alinhadas com os resultados das BIA's?
- Existe documentação para as premissas utilizadas e um racional de classificação por importância do impacto?
- Os *Recovery Time Objetives* (RTO) e os *Recovery Point Obectives* (RPO) estão identificados?

De acordo com a DRI (2018), um RTO é o tempo definido como objetivo para a restauração e recuperação das funcionalidades ou recursos, com base num tempo máximo aceitável que estes podem estar em baixo e o seu nível de desempenho em caso de um evento disruptivo. Já o RPO é definido como o ponto para o qual a informação utilizada por uma atividade deve ser restabelecida, ou de uma forma mais simples, o máximo de informação que pode ser perdida.

Cabe também aos profissionais da gestão de continuidade de negócio e de acordo com a DRI (2018):

- Identificar os critérios qualitativos e quantitativos a serem usados na avaliação do impacto na organização após um evento;
- Obter consenso com a chefia direta sobre a metodologia da análise de impacto de negócio e os critérios utilizados para a definir, bem como, os seus processos;
- Planear e coordenar a recolha de informação e análise a ser feita;
- Estabelecer os critérios e metodologia a serem utilizados na execução das BIA's;
- Analisar a informação recolhida e aplicar os critérios previamente definidos para chegar ao (RTO) e (RPO);
- Preparar e apresentar os resultados das BIA's e obter aprovação do RTO e RPO;

Fases de um PCN

Um PCN tem diversas fases. Desde o momento em que deve ser acionado, até ao momento em que já não está em prática (retorno à normalidade). O *SANS Institute* em 2006 dividiu os PCN em três fases:

- Resposta ao incidente ou fase de ativação;
- Resolução do problema;
- Retorno à normalidade das operações ou fase de recuperação.

Na eventualidade da ocorrência de eventos que ponham em risco o normal funcionamento das operações, o PCN pode ser acionado. O tipo de eventos disruptivos que levam à ativação do PCN, segundo o *SANS Institute* (2006), podem ser:

- Ameaças à segurança dos colaboradores;
- Ameaças à segurança das infraestruturas;
- Ameaças ao ambiente onde a organização está inserida;
- Ameaças a infraestruturas críticas e essenciais para as operações (energia, abastecimento de água, comunicações);
- Ameaças às operações a nível de processos, fornecedores ou parcerias críticas.

O PCN apenas é dado como terminado quando as infraestruturas, serviços ou pessoal afetados voltam a operar dentro da normalidade, ficando concluída deste modo a recuperação.

Gestão de Continuidade de Negócio (GCN)

De acordo com o *IT Governance* (fevereiro, 2019), a Gestão de Continuidade de Negócio (GCN), trata a capacidade de lidar com diversos cenários de interrupção, dispondo de planos de contingência e recursos que possam satisfazer os requisitos exigidos pelos processos definidos nestes planos, de acordo com os objetivos da organização. Estes planos devem ser devidamente documentados e atualizados, por uma equipa competente e responsável pela resposta a eventos disruptivos e recuperação.

A GCN é uma matéria que é especifica para cada organização e que deve ser definida conforme as necessidades de cada caso em específico sendo difícil que existam duas organizações distintas exatamente com as mesmas necessidades e planos implementados. Não existem por modelos que possam ser aplicados de forma integral nas organizações, mas apenas modelos genéricos que devem depois ser adaptados e detalhados de acordo com cada caso.

ISO 22301

A ISO 22301 é uma norma internacional para a GCN e define os requisitos passíveis de serem auditados e certificados, passando uma comunicação positiva para os Clientes e outros *Stakeholders* de garantia que a organização está preparada para responder e recuperar em caso de disrupção.

A ISO 22301 é uma importante fonte de informação sobre procedimentos e conceitos de continuidade de negócio e pode ajudar as organizações a desenvolver sistemas robustos de continuidade de negócio. Esta norma faz uma importante ponte sobre o tema da continuidade de negócio e a função de Auditoria pois a certificação de acordo com os seus requisitos é alvo de diversas formas e fases de auditorias, demonstrando que esta função desempenha um papel fundamental para que possa existir reconhecimento da qualidade dos planos.

Plano de Recuperação de Desastre (PRD)

Para diferenciar um PCN de um PRD, importa definir este último, que segundo o glossário para a resiliência DRI (2018), é um plano que visa a recuperação de um ou mais sistemas num local alternativo como resposta a um evento que tenha causado a interrupção das operações.

Em 2017, o *Business Continuity Institute* (BCI) em parceria com o *Disaster Recovery Journal* (DRJ) no glossário dos termos de PCN, definem *Disaster Recovery* (DR) como o processo, políticas e procedimentos relacionados com a preparação para recuperação e continuidade das infraestruturas tecnológicas, sistemas e aplicações que são vitais para a organização após a ocorrência de um desastre. Como nota é ainda referido que o DR se foca na informação ou sistemas tecnológicos que são a base para o funcionamento da organização, enquanto a continuidade de negócio implica um planeamento que visa manter todos os aspetos essenciais do negócio em funcionamento durante a ocorrência de um desastre. De acordo com o BCI, a "recuperação de desastre" é um subconjunto da "continuidade de negócio".

Ainda no glossário publicado pelo BCI & DRJ, um PRD é definido como um documento aprovado pela gestão de topo, que define os recursos, ações, tarefas e informação necessária para gerir a recuperação da tecnologia. Por norma, refere-se à recuperação de elementos tecnológicos essenciais afetados por um evento disruptivo.

De acordo com o *IT Governance* (março. 2019) a recuperação de desastre enquanto disciplina diferenciada de continuidade de negócio, foca-se na recuperação para as capacidades plenas dos recursos relacionados com SI após um evento disruptivo. Desta forma a recuperação de desastre deve abranger um vasto leque de possíveis eventos disruptivos e para cada um deles uma solução para a recuperação total dos SI. A distinção para a continuidade de negócio está em que esta, não visa apenas recuperação das funcionalidades, mas sim garantias de que no caso de um evento disruptivo as funcionalidades previamente definidas como cruciais, continuam a operar mesmo que a um nível mínimo de capacidade.

Auditoria a Planos de Continuidade de Negócio

Swanson (2013) refere que, auditorias internas à segurança dos SI, PCN e PRD, são altamente recomendadas. A gestão de topo / administrações, devem garantir que efetivamente os planos estão preparados para ser postos em prática em qualquer momento e que a continuidade das operações está assegurada de forma eficaz e eficiente.

Uma análise independente dos PCN ou de recuperação de desastre por parte dos auditores internos pode fornecer informações objetivas sobre a adequação dos programas para prevenirem a não continuidade do negócio em caso de falhas. Os PCN devem ser atualizados ao mesmo ritmo da a evolução do meio envolvente da organização (Swanson, 2013).

Como noutras matérias, a auditoria a PCN é uma função essencial de garantia e obtenção de prova de conformidade dos processos face ao definido inicialmente como objetivo. Bronack (2012), refere que uma auditoria a PCN no âmbito dos SI é essencial e pede verificação aos seguintes elementos:

- A adequação e nível de abrangência do plano;
- A disponibilidade dos processos e das pessoas para implementar o plano;
- Os testes efetuados;
- A verificação das funções diárias necessárias para que o plano possa ser posto em prática a qualquer momento e de forma eficaz.

Bronack (2012) divide os momentos da auditoria a PCN em três grandes componentes:

- Validação do PCN;
- Identificação e validação de medidas preventivas e que visem facilitar a continuidade;
- Análise das evidências sobre o desempenho das atividades que garantem a continuidade e recuperação.

Testes efetuados pela Auditoria

De acordo com Swanson (2013) uma auditoria a PCN pode incluir além de outros, os seguintes testes:

- Entrevistas aos principais *Stakeholders* e participantes dos programas de continuidade;
- Revisão da documentação do projeto, o seu planeamento e outros documentos relacionados com IT;
- Revisão dos planos através da verificação que estes são completos, apropriados e atualizados;
- Verificação dos tempos de recuperação e obtenção de prova de que são possíveis de atingir;
- Examinação da informação obtida nos testes efetuados, procedimentos e comunicações por parte da gestão referentes a situações de BCP ou DR que possam ocorrer e o que os colaboradores devem fazer;
- Revisão dos planos de testes a efetuar e dos resultados dos testes já efetuados;
- Avaliação dos funcionários mais relevantes quanto à sua preparação e conhecimento dos procedimentos;
- Revisão do impacto que novas leis ou regulamentos possam ter nos planos;
- Revisão de contratos e prontidão dos serviços relacionados.

Alguns dos pontos acima referidos pelo autor estarão mais direcionados para auditorias internas, sendo esse o contexto da publicação, podendo, no entanto, serem adaptados para auditorias externas.

Componente empírica

Do trabalho de campo realizado são de relevar e apresentar neste artigo, dois, em formato de entrevista, sendo um deles com um Diretor de Risco Operacional de uma instituição financeira na área da banca a atuar no mercado português. Este contacto é de grande importância para o trabalho de investigação desenvolvido, uma vez que pertence a uma área fortemente regulamentada e auditada, sendo a componente de continuidade de negócio um dos fatores críticos desta regulamentação. O outro entrevistado foi um Diretor de Segurança a nível nacional de uma empresa líder na área da logística a atuar no mercado ibérico.

O método de entrevista foi o método escolhido para esta investigação pois foi uma forma de além de obter algumas respostas utilizadas para este trabalho, foi também uma forma de conseguir a validação das questões abordadas e que serão posteriormente utilizadas para um questionário mais genérico a ser utilizado num trabalho de maior dimensão e profundidade sobre o tema.

A primeira questão abordada relacionou-se com o tema da separação entre a continuidade de negócio e a recuperação de desastre. Ao longo das pesquisas realizadas, embora as principais fontes façam uma clara distinção entre uma matéria e outra, por vezes até, existindo em teoria departamentos separados com o objetivo desta distinção poder ser feita em termos operacionais, as organizações precisam de ter uma estrutura madura e desenvolvida o suficiente para que possam suportar e manter esta separação funcional.

Foi então necessário questionar se as organizações nacionais, consideradas grandes empresas que atuam no mercado, fazem de facto esta distinção. No caso da Banca, o entrevistado garante que não existe uma separação entre as duas funções, nem sequer um departamento exclusivamente responsável pela continuidade de negócio, uma vez que esta responsabilidade assenta no departamento de risco operacional.

No entanto, provavelmente por força das regulamentações e auditorias realizadas, os processos definidos estão de acordo com esta separação e talvez apenas por uma questão de dimensão, não existam pessoas a trabalhar exclusivamente nestes temas. Esta separação é possível de verificar pois existem três cenários possíveis de desastre para os quais a organização está preparada, sendo eles, o desastre físico (incêndio, terramoto, inundação, etc…), cenário de uma pandemia (vírus ou outras doenças contagiosas que ponham em causa a integridade dos colaboradores) e o cenário de desastre tecnológico (ataque informático ou falha dos sistemas).

Desta forma podemos constatar os dois primeiros cenários no âmbito de (PCN) e o último (PRD). No caso da empresa da área da logística, a resposta é mais clara, dando a indicação que esta separação não tem de existir necessariamente e que estas duas matérias são indissociáveis. Possivelmente por este setor não ser tão regulamentado como a Banca, e em princípio a organização não ser auditada nestas matérias, não exista uma maior conformidade com a distinção apresentada e também pelas principais referências bibliográficas.

Outra questão considerada relevante para o artigo foi o envolvimento da gestão de topo / administração na elaboração e testes efetuados no âmbito da continuidade de negócio. Sobre este tema existe conformidade nas respostas, na medida em que a administração deve aprovar os planos elaborados e por isso mesmo está envolvida nos mesmos.

O tema da certificação ISO 22301 foi outro dos assuntos abordados. Sendo consensual a importância desta certificação, ou qualquer outra que influencie as organizações a ter presente a importância dos processos definidos nos planos e dos testes regulares a serem efetuados. Por norma, a pressão de auditorias ou de necessidade de apresentar certificações a terceiros, é o que leva as organizações a estarem melhor preparadas para estes eventos.

Um dos fatores apresentados com importantes no desenvolvimento dos PCN ou PRD são medidas alternativas para eventuais eventos disruptivos em terceiros, cujos serviços sejam essenciais para a organização. Por exemplo, na eventualidade de falha de algum dos principais fornecedores, é importante que a organização esteja preparada para continuar. Este é um ponto que é consensual para os entrevistados. Uma das soluções apresentadas e que está em prática, passa por colocar cláusulas de continuidade diretamente nos contratos com fornecedores.

No seguimento das questões apresentadas, importa referir o tema da hierarquização dos fornecedores por ordem de importância, a constar nos planos a serem desenvolvidos. Embora todos os fornecedores sejam importantes, certamente existe uma parte deles que é facilmente substituída em qualquer altura, mesmo não se tratando de algum evento disruptivo. Outros eventualmente serão mais complicados quanto a alternativas. Desta forma importa que existam planos bem definidos com outras soluções em caso de necessidade.

Uma conclusão importante retirada é a de que esta hierarquização não será, nem deve ser abordada por uma mera observação dos fornecedores, mas sim através de processos considerados cruciais para a organização e por sua vez, quais são os fornecedores que devem estar envolvidos nestes processos.

A regularidade dos testes foi outra das questões respondidas. É possível concluir que estes devem ser efetuados, pelo menos, numa base anual. Um período anual não significa que tenha de ser feito um simulacro igual todos os anos, mas sim um simulacro anual para cada cenário chave, contemplado no plano.

No caso da instituição financeira que tem vários cenários, não será possível testar num único dia todas as possibilidades, podendo estas simulações durarem vários dias, semanas, ou serem repartidos por fases ao logo do ano. Este é um tema que dependerá sempre da complexidade dos planos, bem como, da capacidade que a estrutura da organização tem para suportar estes testes. Uma organização considerada resiliente deverá ter documentadas as evidências dessa resiliência. Claramente este será um dos pontos relacionados e onde devem incidir as auditorias.

Quanto ao conhecimento e envolvimento de todas as pessoas da organização sobre os planos, foi possível observar um grau de maturidade diferente nas respostas das organizações em análise. Enquanto a organização da área da logística indica claramente que apenas as pessoas consideradas chave estão envolvidas, a instituição financeira, embora tenha também um grupo de pessoas chave e com funções mais especificas, indica que todas as pessoas devem ter conhecimento dos planos e da sua missão no caso da ativação dos mesmos.

Os profissionais entrevistados, ambos afirmaram ser de grande importância e além disso, uma exigência, que os planos tenham enumerados os riscos potenciais identificados e a partir destes, a cadeia de ações a pôr em prática aquando da ativação do PCN. Estes riscos potenciais devem estar bem definidos e para além disso, a partir de que nível se devem ativar os planos.

Uma das conclusões retiradas da entrevista com a instituição financeira foi que existem incidentes a ocorrer todos os dias, mas que são em pequena escala e imediatamente resolvidos, não havendo necessidade de ativação dos PCN, ou seja, está claramente definido que apenas a partir de um determinado nível existe essa necessidade.

Outra característica identificada em ambas as organizações é a existência de um mapeamento dos processos por nível de importância, de modo a que fiquem definidos quais os que serão prioritários em caso de ativação dos planos. É importante haver uma hierarquia por importância dos processos a reestabelecer, de modo a que tudo ocorra de forma organizada, sem sobrecarga dos sistemas ou pressão junto dos colaboradores no caso de ocorrerem vários processos a serem iniciados ao mesmo tempo.

Um elemento bastante importante que deve constar nos planos e que certamente deve ser um dos alvos de auditoria, sem o qual estes podem não ter viabilidade, é a articulação com terceiros, sejam eles entidades públicas, clientes, fornecedores ou autoridades. Ambos os entrevistados concordaram com este assunto, sendo que no caso da instituição financeira, por força da regulamentação, têm inclusive a obrigação de comunicação ao Banco de Portugal da ocorrência de qualquer ataque ou desastre que ponha em causa as operações ou segurança dos ativos e eventualmente a ativação do PCN.

Esta comunicação e articulação dos processos com terceiros é de extrema importância, uma vez que não adianta ter, por exemplo, preparados locais alternativos que impliquem deslocação de pessoal, sem que estejam definidas formas de garantir esta deslocação ou que estejam informados os principais interessados (Clientes, fornecedores, autoridades, entre outros) dos novos locais a dar continuidade às operações.

CONCLUSÃO

Sendo a auditoria uma atividade de garantia e de extrema importância, que atesta e garante a conformidade dos resultados com o planeamento inicial, podemos afirmar que o foco desta nos processos de continuidade de negócio, como parte da gestão e mitigação de eventuais riscos, deve ser uma das atividades que não pode ficar esquecida.

Importa, neste âmbito, validar que a continuidade de negócio é uma área considerada de elevada importância para a gestão de topo das organizações e que esta ideia está implementada transversalmente a toda a estrutura. Deve haver uma validação do que são considerados diversos cenários possíveis de risco e que para cada um deles, exista uma solução ou plano de contingência, continuidade ou recuperação em caso de ocorrência.

Uma das matérias que serve de base para estes planos são as BIA's. A qualidade da sua execução influencia todos os processos daí para a frente. É importante por isso verificar que o conjunto de processos e atividades está devidamente documentado e que os requisitos de negócio estabelecidos pelas organizações, estão em conformidade com a sua capacidade de os cumprir.

Uma auditoria deve rever a existência de eventuais certificações, tanto dos planos como um todo, como de profissionais especializados nestas matérias ou até mesmo de entidades externas que prestem serviços nesta área à auditada.

A auditoria para atestar a suficiência dos planos de continuidade deve verificar que a sua abrangência está ao nível das necessidades da organização e eventuais riscos considerados. Importa ainda analisar a documentação retirada dos testes efetuados que comprove a eficácia e estado de prontidão dos mesmos. Dependendo do tipo de auditoria, pode até haver acompanhamento e envolvimento nos testes, se estivermos a falar, por exemplo, de uma auditoria efetuada pela entidade que emite a certificação.

Como um dos processos a executar nos mais diversos tipos de auditoria, as confirmações externas são também neste caso uma mais valia que atesta e valida os processos definidos nos planos. Estas confirmações externas podem ser feitas ao nível dos prestadores de serviços de SI por exemplo, quanto à fiabilidade da segurança da informação e *backups*, ou na articulação com entidades externas nas atividades estabelecidas pelos PCN.

Com este artigo pretendeu-se dar uma ideia clara da importância e definição do tema PCN para as organizações e traçar de uma forma breve aquilo que são as matérias auditáveis neste âmbito, bem como, a importância das auditorias procurando assim ajudar, as equipas e os profissionais, a terem uma abordagem ao problema com mais profundidade.

Complementarmente aos assuntos abordados acrescem ainda os já referidos na parte inicial do artigo. Em regra, os conteúdos e os relatos, foram obtidos de forma estritamente confidencial. A investigação está ainda em desenvolvimento, terá certamente um maior detalhe numa dissertação mais extensa e que se encontra a decorrer.

Acresce ainda referir que estão a ser utilizadas outras técnicas e métodos de investigação. Desde logo, o método dedutivo e o método indutivo, a nível nacional, que irão permitir estabelecer a relação entre as práticas em vigor com aquilo que são as recomendações das principais entidades de regulamentação internacionais sobre o tema continuidade de negócio.

Por fim damos conta de alguns temas que não puderam ser abordados neste artigo e que também merecem referência por fazerem parte da investigação a decorrer. São eles a relação entre os eventos diruptivos e a mitigação do risco através de apólices de seguro já identificadas, bem como, a existência de certificações importantes para os profissionais enquanto especialistas nestas áreas, algo que na realidade nacional não aparenta um propósito ou ser de fácil identificação, mas que podem realmente acrescentar valor aos Clientes que comunicam com as diversas áreas funcionais num alinhamento aos processos de negócio existentes.

Referências Bibliográficas

BCI & DRJ (2017) *Glossary of Business Continuity Terms,* disponível em https://www.thebci.org/asset/E6E7B9C3-355F-49D9-80340124B2E836E8

Bronack, T. (2012). *Auditing a BCP Plan,* disponível em http://www.dcag.com/images/AUDITING_A_BCP_PLAN.pdf

Disaster Recovery Institute International (DRI). (2018) *Glossary for Resilience,* disponível em https://drii.org/glossarydocdowload/english/International_Glossary_for_Resilience_2018

Disaster Recovery Institute International (DRI). (2018) *The Professional Practices for Business Continuity Management*, disponível em https://drii.org/resources/professionalpractices/EN

ISO 22300 (2018). *Security and resilience – Vocabulary*, disponível em https://www.iso.org/obp/ui/#iso:std:iso:22300:ed-2:v1:en

IT Governance (Fev. 2019), *Business Continuity Management*, disponível em https://www.itgovernance.co.uk/resources/green-papers/business-continuity-management-the-nine-step-appro

IT Governance (Mar. 2019), *Business Continuity and ISSO 22301*, disponível em https://www.itgovernance.co.uk/resources/green-papers/business-continuity-management-iso22301-faq

Jorrigala, V. D. (2018), *Business Continuity and Disaster Recovery Plan for Information Security*, disponível em https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article= 1068&context=msia_etds

KPMG (2006). *Building a Continuity Culture*, disponível em http://www.dcag.com/images/BusinessContinuity.pdf

KPMG (2016). *Business Continuity Management*, disponível em https://assets.kpmg/content/dam/kpmg/pdf/2016/06/hu-business-continuity-management.pdf

Swanson, D. (2013) *How to Audit Business Continuity Program*, disponível em https://info.knowledgeleader.com/bid/187874/how-to-audit-business-continuity-programs

Anexo 5 Participação em eventos, seminários, webinar's entre outros que contribuíram para a investigação

Participação no congresso: XIII Congresso dos ROC "Auditoria – Novos Caminhos". Realizado em 12/09/2019

Participação no seminário: A transformação digital e o impacto na Contabilidade, na Ordem dos Contabilistas Certificados. Realizado em 26/09/2019

Participação no webinar: *COVID-19 & Shared Services Webinar: Redefining BCP & Service Delivery Models to Protect Against Future Threats, por Shared Services and Outsourcing Network (SSON).* Realizado em 26/03/2020

Participação no webinar: *SSON's Business Continuity Planning Digital Summit 2020*. Realizado em 23/04/2020

Participação no evento: Missão e visão do Governo no quadro da Estratégia de Segurança Nacional de Segurança do Ciberespaço, aprovada por Resolução de Conselho de Ministros, evento do ISCAL em que foi recebida a Dra. Isabel Baptista, coordenadora do Departamento de Desenvolvimento e Inovação do Centro Nacional de Cibersegurança. A apresentação foi disponibilizada pela oradora. O evento foi organizado no âmbito do Mestrado em Auditoria com a organização do docente do ISCAL Fernando Rodrigues. Realizado em 14/05/2020