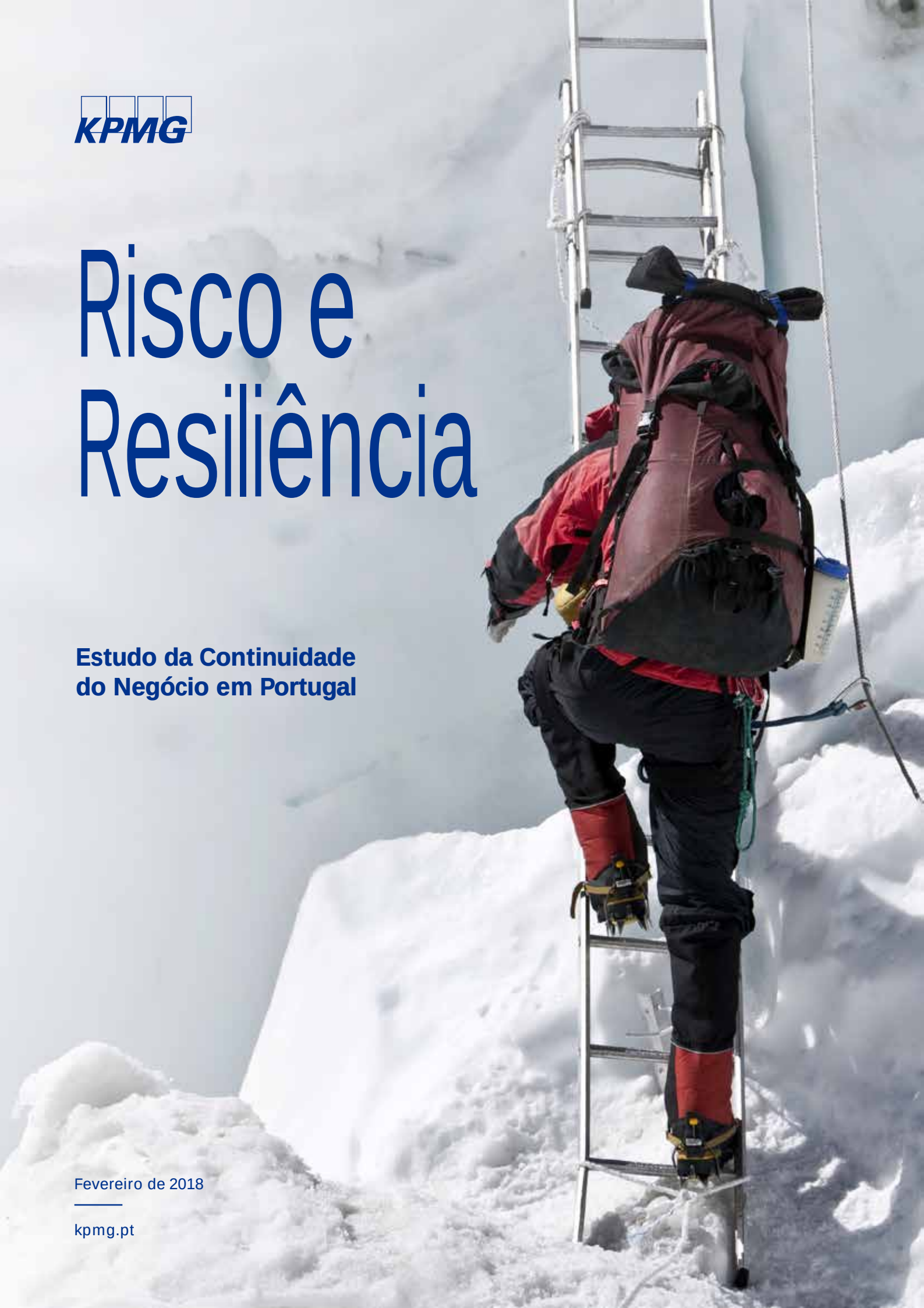


Risco e Resiliência

Estudo da Continuidade do Negócio em Portugal

Fevereiro de 2018

kpmg.pt

Bem-vindo ao Estudo da Continuidade do Negócio em Portugal, uma iniciativa da KPMG em Portugal, que apresenta uma análise detalhada sobre os riscos relacionados com eventos disruptivos e os mecanismos de resiliência implementados em Organizações representativas de sectores chave para a economia portuguesa.

O estudo foi realizado entre Setembro e Novembro de 2017, através de dois questionários electrónicos – Gestão da Continuidade do Negócio e Gestão da Continuidade de Serviços de Tecnologias de Informação – respondidos por 76 gestores responsáveis por estas funções nas suas Organizações e entrevistas com quatro Administradores executivos com o pelouro da Continuidade do Negócio.

Vivemos num mundo digital, as novas tecnologias abrem novos horizontes mas trazem também novos riscos para as Organizações, pelo que não é de estranhar que no topo da lista de preocupações dos gestores da Continuidade do Negócio estejam os incidentes de Cibersegurança e a falha das Tecnologias de Informação, com grande destaque em comparação com outros eventos de risco como a falha dos fornecedores críticos da cadeia de valor, a falha de *utilities* ou incêndios, terrorismo e desastres naturais.

As transformações tecnológicas, climatéricas, sociais, políticas e económicas forçam as Organizações a tornarem-se mais ágeis e proactivas na prevenção e resposta às novas ameaças emergentes. Assim, a quase totalidade das Organizações afirma possuir algum nível de resiliência, ou seja, implementaram controlos preventivos para reduzir a exposição aos riscos relevantes para a sua actividade e mecanismos para recuperar as suas funções críticas no seguimento de um incidente disruptivo, o que nos permite concluir que a Continuidade do Negócio está já enraizada na sua cultura.

A Gestão da Continuidade do Negócio é cada vez mais um tema na agenda dos Conselhos de Administração. Na maioria das Organizações a função é da responsabilidade do Presidente do Conselho de Administração, mas pode estar também atribuída a Administradores com o pelouro das Tecnologias de Informação, Gestão do Risco ou Segurança.

As Organizações implementam os seus programas de Gestão da Continuidade do Negócio seguindo recomendações da legislação sectorial nesta matéria, normas internas corporativas e a norma de referência ISO 22301 que estabelece os requisitos de certificação de um Sistema de Gestão da Continuidade do Negócio. A norma ISO 22301 é seguida como uma boa prática, independentemente da Organização pretender vir a obter a certificação ou não.

Os planos, soluções e testes de IT *Disaster Recovery* continuam a ser as áreas de maior foco nos programas de Gestão da Continuidade do Negócio. No entanto, as Estratégias da Continuidade dos Serviços de TI não estão frequentemente integradas e alinhadas com as Estratégias de Continuidade do Negócio, sendo claramente um aspecto a melhorar nas Organizações.

A KPMG agradece o contributo dos gestores que amavelmente partilharam informação valiosa sobre a Continuidade do Negócio e a Continuidade dos Serviços de TI nas suas Organizações.

Os profissionais da KPMG estão empenhados em contribuir para o aumento da resiliência das empresas portuguesas e estão à sua disposição para discutir os desafios da Continuidade do Negócio na sua Organização.

Nasser Sattar
Head of Advisory

Índice

Introdução

A Gestão da Continuidade do Negócio e a Continuidade dos Serviços de TI são processos de gestão essenciais para assegurar a resiliência das Organizações a eventos disruptivos que possam afectar a sua actividade.

A Gestão da Continuidade do Negócio tem como objectivo identificar ameaças potenciais, analisar o impacto dessas ameças no negócio caso se venham a concretizar e implementar a resiliência organizacional de forma a prevenir a sua ocorrência ou, na sua impossibilidade, responder de forma eficaz a essas ameaças, recuperando rapidamente a normalidade após uma disrupção, minimizando perdas financeiras, danos reputacionais e quebra de obrigações contratuais, legais e regulamentares.

A implementação de um programa de Gestão da Continuidade do Negócio (assinalado a vermelho na figura abaixo) baseia-se na realização das seguintes actividades:

- Análise de Impacto no Negócio: identificar funções críticas, determinar os impactos da sua indisponibilidade e os seus prazos de recuperação para minimizar estes impactos;
- Avaliação do Risco: identificar, analisar e avaliar a exposição ao risco relacionado com eventos disruptivos;
- Estratégia da Continuidade do Negócio (CN): definir soluções de recuperação das funções críticas nos prazos definidos na Análise de Impacto no Negócio e controlos preventivos para reduzir a exposição ao risco relacionado com eventos disruptivos;
- Planos de CN: documentar os procedimentos de resposta a incidentes e de recuperação das funções críticas; e
- Exercícios e Testes de CN: exercitar as pessoas envolvidas na resposta a incidentes e testar as soluções de recuperação das funções críticas.

A implementação de um Sistema de Gestão da Continuidade do Negócio (SGCN) no referencial da norma de certificação ISO 22301, permite às Organizações manter actualizado e melhorar a eficácia do seu programa de Gestão da Continuidade do Negócio através de um modelo cíclico denominado PDCA (*Plan-Do-Check-Act)* que inclui as seguintes actividades, apresentadas na figura abaixo:

- *Plan* - Planear: compreender o contexto, assegurar a liderança e o compromisso da Administração, definir os objectivos e planear a CN;
- *Do* - Implementar e Operar: processo assinalado a vermelho na figura abaixo e já descrito acima;
- *Check* - Monitorizar e Rever: monitorizar e rever o desempenho do SGCN em relação à política e objectivos da Continuidade do Negócio e reportar à Administração; e
- *Act* - Manter e Melhorar: manter e melhorar o SGCN através de acções correctivas, baseadas nos resultados da revisão pela Administração.

Fonte: Baseado no modelo Plan-Do-Check-Act da norma ISO 22301

A Continuidade dos Serviços de TI é uma componente da Gestão da Continuidade do Negócio que consiste na capacidade de uma Organização manter as funções críticas do negócio através da prevenção, detecção, resposta e recuperação de incidentes disruptivos, provocados por eventos de naturezas diversas, que possam afectar o normal funcionamento das TI.

A Continuidade dos Serviços de TI é uma temática endereçada por vários referenciais internacionais. O COBIT 5 endereça esta temática no processo DSS 04 *Manage Continuity* e o ITIL no processo IT *Service Continuity Management.* Ambos os referenciais referem a necessidade de alinhamento com o programa Gestão da Continuidade do Negócio e incluem a recuperação dos Serviços e infra--estruturas de TI.

A norma ISO 27031 estabelece orientações para as Organizações prepararem as suas Tecnologias de Informação e Comunicação para a Continuidade do Negócio (*Information and Communication Technology Readiness for Business Continuity* ou IRBC) incluindo a recuperação da infra-estrutura tecnológica, tipicamente denominada IT *Disaster Recovery* (IT DR), mas também a recuperação dos Serviços de TI, em alinhamento com os requisitos do SGCN no referencial ISO 22301.

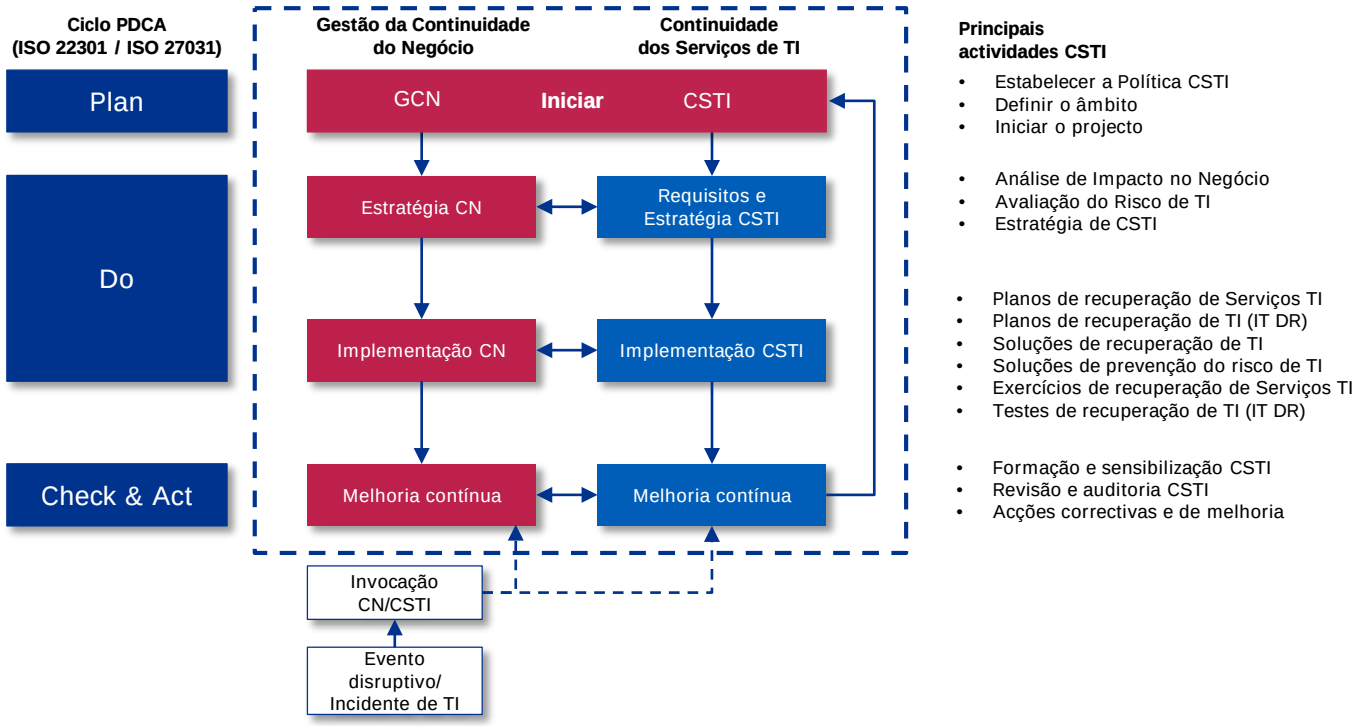
A figura abaixo apresenta a relação entre as actividades de Continuidade dos Serviços de TI do modelo ITIL e o ciclo PDCA das normas ISO.

Assim, a Continuidade dos Serviços de TI vai além do tradicional IT *Disaster Recovery* e endereça um conjunto de elementos chave para os Serviços de TI:

- Pessoas: Especialistas com competências para a operação, manutenção e recuperação das TI;
- Instalações: Instalações físicas onde se encontram os recursos de TI;
- Tecnologia: Aplicações, dados, sistemas e comunicações que suportam funções críticas do negócio e Serviços de TI;
- Processos: Processos que permitem operar, manter e recuperar as Tecnologias de Informação; e
- Parceiros e prestadores de serviços: Entidades externas das quais se está dependente para a entrega dos Serviços de TI (*e.g.* serviços de internet, serviços *cloud,* serviços de *outsourcing de* TI).

O estudo da Continuidade do Negócio em Portugal tem como objectivo obter um panorama global sobre a Gestão da Continuidade do Negócio e a Continuidade dos Serviços de TI em vários sectores da economia portuguesa.

O estudo contou com a participação de gestores responsáveis pela Gestão da Continuidade do Negócio e de gestores responsáveis pela Continuidade dos Serviços de TI. Este relatório apresenta as suas visões sobre estas temáticas nas suas respectivas Organizações.



Fonte: Baseado no modelo ITIL Service Design – IT Service Continuity Management

Conclusões

Risco e resiliência (questionário GCN – dirigido a gestores da CN)

90% estão preocupados com Incidentes de Cibersegurança e **83%** com a Disrupção das TIC

78% estão preocupados com a falha de fornecedores críticos da cadeia de valor, **71%** com a falha de *utilities*, **71%** com incidentes de saúde e segurança no trabalho, **66%** com incêndios, **56%** com terrorismo e **46%** com desastre naturais

98% afirmam ser Resilientes ou algo Resilientes, e implementaram:

- controlos preventivos para redução da sua exposição ao risco,
- mecanismos de resposta a incidentes, e
- soluções de recuperação das funções críticas dentro dos prazos estabelecidos pelo negócio para minimizar impactos financeiros, reputacionais e legais.

Liderança e compromisso (questionário GCN – dirigido a gestores da CN)

33% atribuiram a liderança da Gestão da Continuidade do Negócio ao Presidente do Conselho de Administração, **21%** ao Administrador de TI, **19%** ao Administrador de Gestão do Risco, **9%** ao Administrador de Segurança de Informação e Segurança Física

44% atribuiram a liderança da Gestão da Continuidade do Negócio à Direcção de Gestão de Risco, **17%** à Direcção de TI, **17%** à Direcção de Organização, Qualidade e Ambiente, **10%** à Direcção de Segurança de Informação e Segurança Física

68% dos Administradores aprovam a Política da Continuidade do Negócio

76% possuem equipas dedicadas com competências em GCN

51% dos Administradores presidem ao Comité da Continuidade do Negócio

23% adquiriram competências em GCN através de cursos de formação nos requisitos da norma ISO 22301

51% dos Administradores lideram os exercícios de Gestão de Crise

Continuidade do Negócio (questionário GCN – dirigido a gestores da CN)

59% implementaram um Sistema de Gestão da Continuidade do Negócio e destes, **42%** certificaram ou pretendem certificar o seu SGCN no referencial da norma ISO 22301

56% realizam Análises de Impacto no Negócio em conjunto com avaliações do risco e **49%** definem uma Estratégia de CN com soluções de recuperação das funções críticas dentro dos prazos estabelecidos pelo negócio para minimizar impactos e controlos preventivos para reduzir o risco

88% implementaram soluções de IT DR, **63%** trabalho remoto e **60%** postos de trabalho em instalações alternativas para recuperar as funções críticas dentro dos prazos estabelecidos pelo negócio para minimizar impactos

75% possuem planos de IT DR, **73%** planos de Resposta de Emergência, **63%** planos de Gestão de Crise, **60%** planos de Recuperação do Negócio e **53%** planos de Recuperação dos Serviços de TI

63% realizam testes de IT DR, **59%** realizam exercícios de Recuperação do Negócio e **38%** realizam exercícios de Gestão de Crise, com periodicidade anual ou inferior

64% monitorizam e avaliam os seus programas de Gestão da Continuidade do Negócio através de Auditorias Internas, **41%** através da revisão pela Administração, **38%** através de auditoria externa e **38%** através de indicadores (KPIs)

Continuidade dos Serviços de TI (questionário CSTI – dirigido a gestores de CSTI)

71% sofreram um incidente que causou a indisponibilidade dos Serviços de TI nos últimos cinco anos

54% tiveram os serviços de TI indisponíveis por mais de 4 horas, **34%** de 4 a 8 horas, **8%** entre 4 e 24 horas, **8%** entre 24 e 48 horas e **4%** entre 48 e 72 horas

44% foram afectados com falhas de comunicações, **41%** com falhas de energia, 38% com falha de hardware, **29%** com falha de software e **24%** com ataques de vírus/*malware*/*ransomware*

26% possuem uma Estratégia da Continuidade dos Serviços de TI alinhada e integrada com a Estratégia da CN

59% possuem planos de Recuperação dos Serviços de TI e **50%** implementaram soluções de recuperação para todos os processos críticos de TI

97% possuem planos e implementaram soluções de IT DR e **57%** cobrem todas as aplicações críticas do negócio

56% das soluções de IT DR estão alojadas no *Data Centre* alternativo próprio, **29%** num *Data Centre* alternativo de um prestador de serviços, **24%** recorre a soluções *Cloud* Privada num prestador de serviços e apenas **6%** recorre a *Cloud* Pública

59% realizam testes de IT DR recuperando todas as aplicações críticas dentro dos RTOs e RPOs

Risco e Resiliência

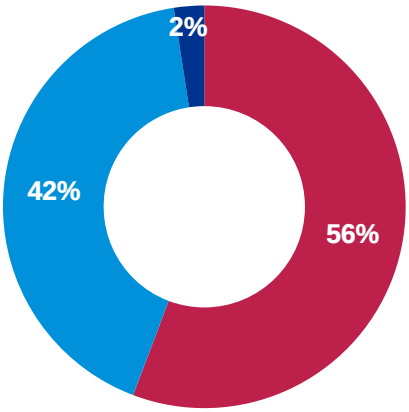
Vivemos numa época em que proliferam eventos que podem colocar em risco a Continuidade do Negócio nas Organizações. A melhor estratégia para gerir o risco de uma interrupção prolongada das funções críticas do negócio é esperar o inesperado e estar preparado para lidar com qualquer evento que possa provocar um incidente disruptivo.

A Gestão da Continuidade do Negócio visa implementar a resiliência organizacional, isto é, a capacidade para prevenir, responder e recuperar de incidentes disruptivos, provocados por eventos de naturezas diversas, que possam afectar o normal funcionamento das funções críticas do negócio, minimizando perdas financeiras, danos reputacionais e quebra de obrigações contratuais, legais e regulamentares.

A quase totalidade das Organizações que participou neste estudo (98%) implementou mecanismos para assegurar a resiliência organizacional. Neste universo, 56% das Organizações afirmam ser resilientes e 42% afirmam ser algo resilientes, o que permite concluir que a Continuidade do Negócio está já enraizada na sua cultura.

Mário Vaz, CEO da Vodafone Portugal explica o impacto de uma interrupção de serviços para os seus clientes "Somos uma empresa de comunicações para a sociedade, para os indivíduos e para as empresas e no mundo em que vivemos hoje as comunicações são essenciais. Uma interrupção nos nossos serviços pode privar milhões de pessoas de comunicações de voz, dados, serviços de televisão e pode

Gráfico 1: Percepção de resiliência



Resiliente
Foram implementados controlos preventivos para reduzir a exposição aos riscos mais relevantes para a sua actividade, mecanismos de resposta a incidentes e soluções para recuperar as funções críticas dentro dos prazos estabelecidos pelo negócio para minimizar impactos

Algo Resiliente
Foram implementados alguns controlos preventivos para reduzir a exposição a alguns riscos relevantes para a sua actividade, alguns mecanismos de resposta a incidentes ou algumas soluções para recuperar funções críticas

Não Resiliente
Não foram implementados controlos preventivos para reduzir a exposição aos riscos mais relevantes para a sua actividade, nem mecanismos de resposta a incidentes nem soluções para recuperar as funções críticas

Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

> Para nós, Continuidade do Negócio é o nosso dia-a-dia, garantindo que os nossos clientes não têm interrupções nos seus negócios.

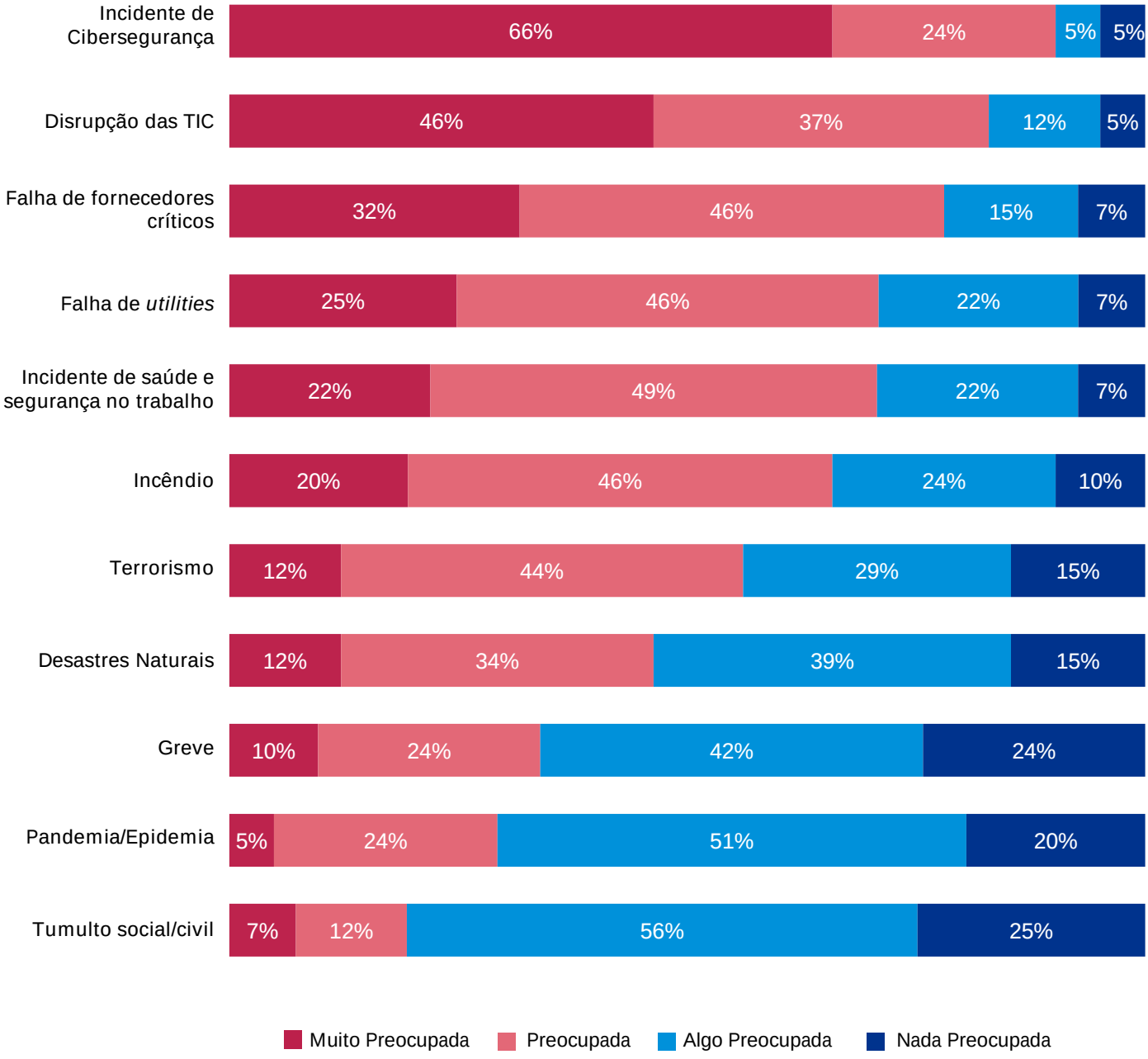
Mário Vaz
CEO
Vodafone Portugal

afectar a produtividade das empresas que têm contratados serviços de comunicações, serviços *Cloud* e outros serviços de Sistemas de Informação." O gestor acrescenta a sua percepção de resiliência organizacional: "Num negócio que não pode ter descontinuidade, resiliência significa ter um plano para reposição dos serviços que prestamos aos nossos clientes se um risco que não conseguimos controlar, prever ou evitar se vier a concretizar. A natureza do nosso negócio obriga a actualizar e testar frequentemente os objectivos de recuperação por tipo de serviço, e a Vodafone Portugal assume este compromisso. Portanto, considero que a Vodafone Portugal é uma Organização resiliente, sem dúvida nenhuma."

João Torres, CEO da EDP Distribuição, partilha a sua visão: "A EDP Distribuição é a entidade em Portugal Continental responsável pela Rede Nacional de Distribuição. A nossa actividade tem hoje um impacto nas pessoas e na energia de Portugal que a torna particularmente exigente no seu desempenho". João Torres acrescenta: "A resiliência da Organização reflecte-se na gestão diária da nossa actividade. Perseguimos os alinhamentos estratégico, táctico e operacional estabelecidos, através da implementação efectiva das melhores práticas, tendo por objectivo proporcionar a disponibilidade dos serviços críticos da empresa, o mais rapidamente possível, após uma disrupção. A resiliência organizacional é um processo de aprendizagem e de melhoria contínua dinâmico, que se desenvolve passo a passo e ao longo do tempo, reconhecendo que este é um desafio de mudança cultural."

João Luis Baptista, COO da SIBS, faz também a sua análise: "A SIBS assegura o *backbone* transaccional do ecossistema financeiro português, quer ao nível dos utilizadores finais (nacionais e internacionais) quer ao nível da Banca. Qualquer disrupção dos nossos serviços teria, portanto, fortes impactos no dia-a-dia dos seus utilizadores, que realizam diariamente mais de sete milhões de operações através dos sistemas da SIBS. Do simples levantamento de dinheiro ao pagamento das compras num supermercado, do pagamento da factura da água ao pagamento de impostos, do pagamento de uma compra na internet ao pagamento da portagem, qualquer falha por pequena que seja, teria impactos sérios na economia nacional." João Luis Baptista não tem dúvidas quanto à resiliência da SIBS; "Desde o primeiro dia que a SIBS tem realizado diversos investimentos na resiliência e fiabilidade dos seus serviços, que apresentam um nível de *uptime* na ordem dos 99,9%."

Gráfico 2: Nível de preocupação com eventos de risco



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

As Tecnologias de Informação desempenham um papel fundamental para assegurar a vantagem competitiva dos negócios, mas são também um importante factor de risco para as Organizações. Os resultados deste estudo colocam os incidentes relacionados com as Tecnologias de Informação no topo da lista de preocupações. 90% das Organizações está preocupada com incidentes de Cibersegurança e 83% está preocupada com a disrupção das Tecnologias de Informação.

O estudo revela que as Organizações estão também preocupadas com a falha de outros recursos fundamentais para as suas operações: 78% das Organizações está preocupada com a falha de fornecedores críticos da cadeia de valor, 71% das Organizações está preocupada com a falha de *utilities* tais como a electricidade, gás e água e 71% das Organizações está preocupada com incidentes de saúde e segurança no trabalho.

Logo em seguida as Organizações estão preocupadas com incidentes do ambiente envolvente que podem surgir de forma inesperada, 66% está preocupada com incêndios, 56% está preocupada com terrorismo e 46% estão preocupadas com desastres naturais.

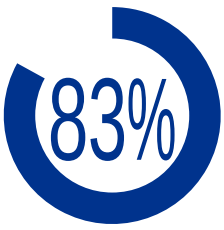
"Os eventos de risco de maior preocupação são muito dinâmicos porque grande parte dos riscos, como ataques terroristas ou catástrofes naturais, vêm do exterior e são imprevisíveis, mas no mundo digital em que hoje vivemos estamos essencialmente preocupados com a entrada maliciosa nos nossos sistemas e com o acesso não autorizado a dados pessoais. É a estas áreas que temos dedicado maior atenção." afirma **Mário Vaz, CEO da Vodafone Portugal**.

João Torres, CEO da EDP Distribuição, refere alguns episódios vividos pela sua Organização: "Os eventos disruptivos com impacto significativo na actividade da EDP Distribuição estão normalmente associados a causas naturais, caracterizados por ventos extremos que provocam inúmeras avarias em simultâneo na rede eléctrica aérea de Média Tensão, como as tempestades do Oeste em 2009; o tornado em Silves em 2012; a tempestade Gong em 2013 que se estendeu a todo o território continental com particular impacto na zona de Pombal e Leiria; a tempestade Stephanie em 2014; a inundação em Albufeira em 2015; a tempestade Dóris, que ocorreu na zona do Minho em 2017. Embora de menor impacto para a infra-estrutura eléctrica, referem-se ainda os incêndios de Góis em 2013, de Arouca-Paiva em 2016 e o incêndio de Pedrógão Grande em 2017, com grande cobertura mediática. Adicionalmente, embora os sistemas do Grupo EDP e da EDP Distribuição não tenham sido afectados, destaco o episódio da ameaça de *ransonware* em Maio de 2017 com o ataque malicioso do *WannaCry*. Constitui, de facto, um dos cenários de risco muito relevante e de importância crescente para o sector da energia, pela transformação digital e crescente automação na monitorização e supervisão da rede, suportada nas redes de comunicações. São enormes desafios ao nível da Segurança da Infra-estrutura de Informação Crítica (IIC) da Rede de Distribuição, quer na sua configuração convencional quer na geração distribuída."

Pedro Cid, Director Geral da Auchan Portugal, revela os principais factores de risco a que a Auchan está exposta: "Estamos muito dependentes da cadeia de abastecimento – fornecedores e logística – e, nas lojas, dos Sistemas de Informação, que asseguram segurança e protecção e que hoje em dia são cruciais e, naturalmente, também dos nossos colaboradores. Temos tido alguns pequenos incidentes – inundações, falhas do sistema informático – mas cujas interrupções no negócio foram sempre de curta duração." E acrescenta "A Auchan considera que é resiliente, ou seja, tem controlos preventivos para evitar os incidentes, redundâncias e mecanismos de gestão de crise e de resposta aos incidentes. A resiliência é uma questão de princípio, de ADN. A Auchan é um grupo que salvaguarda muito bem o seu património."

João Luis Baptista, COO da SIBS, separa os riscos em duas vertentes: riscos de segurança e riscos de continuidade: "No topo das preocupações dos riscos de segurança estão as vertentes de vulnerabilidade a ataques maliciosos e a falta ou deficiente segurança física/lógica. No que diz respeito aos riscos de continuidade, a SIBS está focada na capacidade de recuperar os serviços rápida, eficiente e totalmente; quanto mais aperfeiçoada estiver esta capacidade da empresa, menor será o impacto de um evento disruptivo quer no negócio, quer nos clientes."

das Organizações está preocupada com incidentes de Cibersegurança



das Organizações está preocupada com disrupção das TIC

Liderança e Compromisso

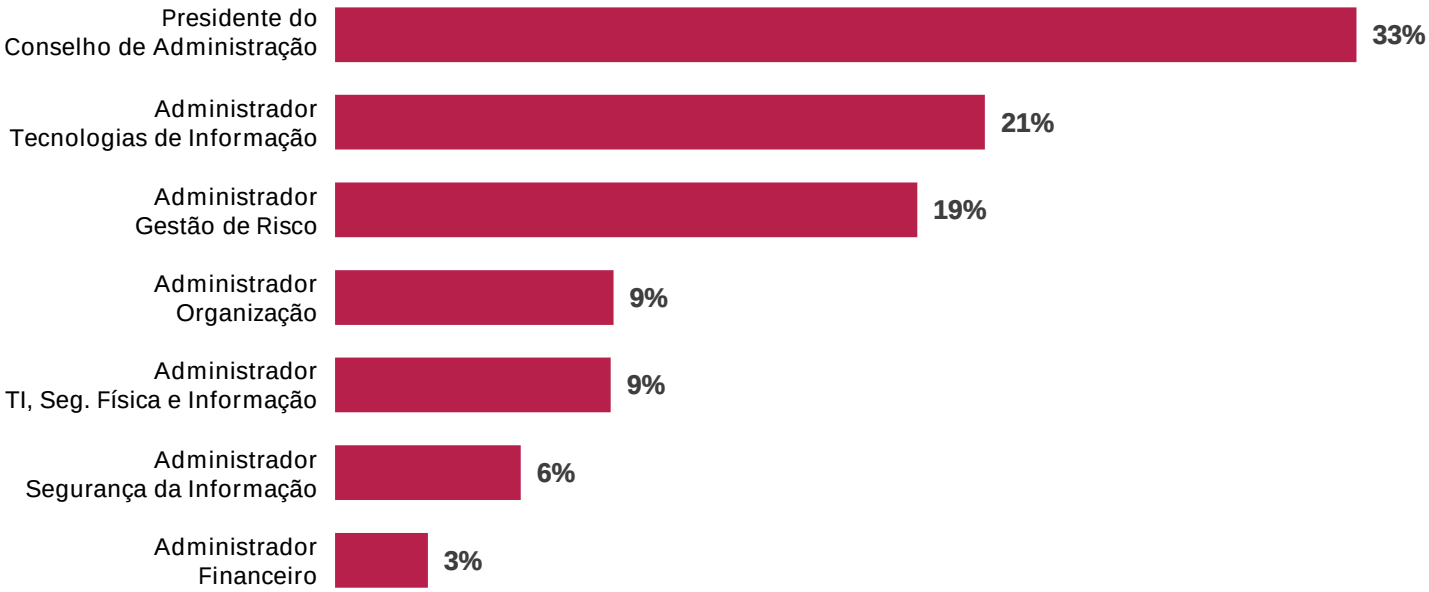
A liderança e o compromisso da Administração são fundamentais para assegurar os recursos e mobilizar a Organização para a implementação e melhoria contínua de um programa de Gestão da Continuidade do Negócio.

Um terço das organizações que participou neste estudo (33%) atribuiu a liderança da Gestão da Continuidade do Negócio ao Presidente do Conselho de Administração, assumindo tratar-se de uma função corporativa transversal à Organização.

Mas a liderança da Gestão da Continuidade do Negócio pode estar também atribuída ao Administrador com o pelouro da área que lidera a sua implementação na Organização. Assim, 21% das organizações atribuiu esta função ao Administrador responsável pelas Tecnologias de Informação e 19% ao Administrador responsável pela Gestão de Risco.

Em organizações com Sistemas de Gestão da Continuidade do Negócio certificados, a gestão de topo deve obrigatoriamente aprovar a política da Continuidade do Negócio, participar em exercícios e efectuar regularmente a revisão do desempenho do sistema de gestão, através da análise de indicadores e dos relatórios dos exercícios e testes e dos relatórios da auditoria interna, assegurando a sua melhoria contínua. Estas práticas são já uma realidade em muitas organizações que não pretendem obter a certificação.

Gráfico 3: Liderança da Gestão da Continuidade do Negócio



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

João Torres, CEO da EDP Distribuição, salienta o papel do Conselho de Administração no Sistema de Gestão da Continuidade do Negócio da EDP Distribuição, certificado no referencial da norma ISO 22301: “Foi uma decisão do Conselho de Administração criar a área de Continuidade do Negócio integrada na Direcção de Ambiente, Sustentabilidade e Continuidade do Negócio. Lembro-me perfeitamente de ter desafiado dois a três jovens que não dominavam o tema a iniciarem este desafio. Ganhámos um prémio do Business Continuity Institute (BCI), ‘Most Effective Recovery of the Year’, na sequência do bom desempenho que tivemos na reacção à tempestade Gong em Janeiro de 2013. De seguida, o desafio foi obter a certificação, o que nos levou a identificar os nossos *gaps* e a melhorar.“ E acrescenta: “Hoje, existe um comité de Continuidade do Negócio em que eu estou presente. A certificação foi acompanhada de muito perto por nós, e fazemos sempre questão de apresentar os resultados ao Conselho de Administração, identificando os *gaps* e as oportunidades de melhoria. Enquanto Conselho de Administração tentamos dar visibilidade ao tema e à área, dentro da Organização. Por exemplo, quer o prémio recebido do BCI, quer a certificação obtida foram questões abordadas nas nossas reuniões trimestrais de balanço, nas quais demos a palavra a quem liderou estes processos. O Conselho de Administração trabalha em várias frentes, mas esta área até por ser recente e pela sua relevância, é uma área muito acarinhada. O Conselho de Administração, e eu em particular, sou muito sensível ao tema, e pela minha experiência e pelas várias conferências em que participei, onde são discutidos estes temas, consigo perceber que é um tema que tem de estar em cima da mesa.”

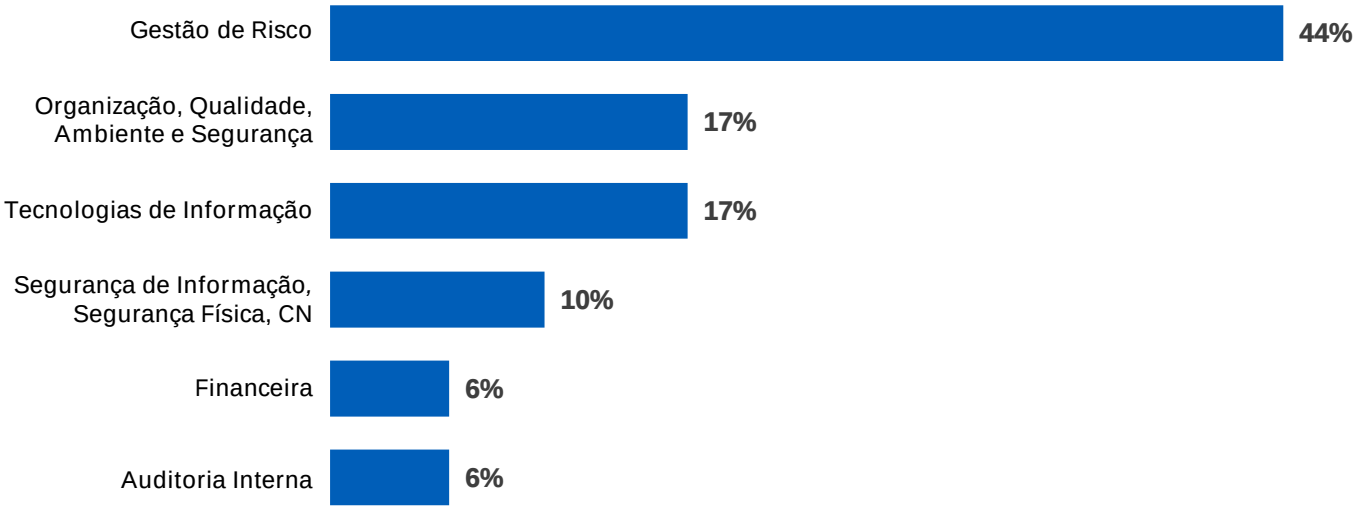
João Luis Baptista, COO da SIBS, explica também o seu papel como representante desta função no Conselho de Administração: “Como administrador com o pelouro pela Gestão da Continuidade do Negócio sou mantido regularmente informado sobre a implementação e resultados da mesma. São registados e analisados vários indicadores e produzidos relatórios que permitem validar a eficácia do programa, sendo os mesmos revistos com regularidade face à sua obsolescência e eficácia.”

Pedro Cid, Director Geral da Auchan Portugal, explica o seu envolvimento no programa de Gestão da Continuidade do Negócio: "A área que lidera a Continuidade do Negócio é a Direcção de *Performance*, que inclui as funções de Auditoria, Controlo Interno, Segurança e Controlo de Gestão. Existe um comité de Segurança, do qual eu sou o Presidente e, desta forma, tenho um envolvimento directo nos programas e na implementação das soluções. No comité de Segurança, que reúne de três em três meses, o Director de Segurança apresenta um balanço sobre os indicadores de desempenho e os resultados das auditorias e dos exercícios e identificamos as vulnerabilidades e as acções correctivas e oportunidades de melhoria para colmatar estas vulnerabilidades. Participo também nos exercícios de Gestão de Crise e nos simulacros, que incluem sempre uma evacuação, e no fim, realizamos uma sessão de *debriefing* e ponto de situação."

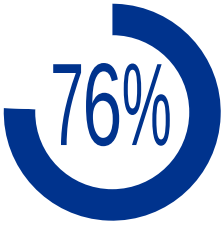
Mário Vaz, CEO da Vodafone Portugal, explica a realidade da Vodafone: "A área que lidera a Continuidade do Negócio é a Direcção de Risco e *Compliance*, que reporta directamente a mim, o que revela a importância do tema no grupo Vodafone "e acrescenta o seu envolvimento pessoal no tema: "Só o facto de reportar directamente já é sinónimo do envolvimento pessoal do CEO. O programa da Continuidade do Negócio inclui planos e soluções que são testados regularmente e estou presente no programa no qual tenho a responsabilidade, entre outras, de liderar a equipa de Gestão de Crise que procura validar a tal resiliência que referi anteriormente."

João Luis Baptista, COO da SIBS, salienta a relevância desta função na SIBS: "Como área absolutamente estratégica para a SIBS, a Gestão da Continuidade do Negócio está sob o meu pelouro e é assegurada pela área de Estratégia e Planeamento do Departamento de Sistemas de Informação."

Gráfico 4: Direcção responsável pela Gestão da Continuidade do Negócio



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal



Três em cada quatro Organizações (76%) possuem equipas dedicadas com competências em Gestão da Continuidade do Negócio

Quase metade das Organizações que participou neste estudo (44%) atribuiu a liderança da Continuidade do Negócio à Direcção de Gestão de Risco, o que reflecte o facto de esta função mitigar o risco de interrupção das operações críticas do negócio.

No entanto, é também comum que esta função esteja atribuída a uma área de Organização, Qualidade, Ambiente e Segurança (17%), que são responsáveis pelo catálogo de processos da Organização e pelos programas de certificação no referencial das normas ISO, ou à área de Tecnologias de Informação (17%), responsável pelos programas de Continuidade dos Serviços de TI.

A função pode estar também atribuída a áreas responsáveis pela Segurança (10%), como é o caso da área de Segurança Física, responsável pela gestão de emergências, evacuação dos edifícios e soluções de prevenção de incidentes nas instalações (e.g. incêndios, inundações), e a área de Segurança de Informação, responsável pelas soluções de prevenção e recuperação de incidentes de Cibersegurança.

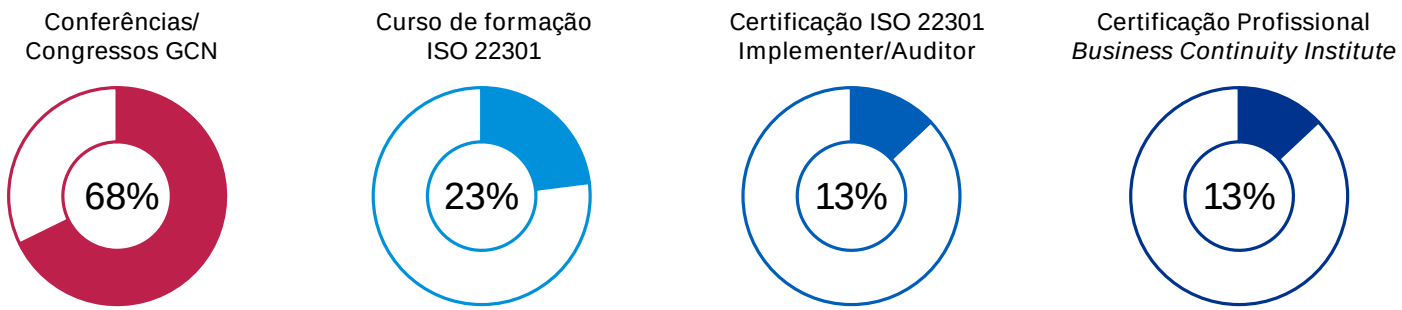
A implementação de um programa de Gestão da Continuidade do Negócio deve assegurar a existência de uma equipa interna com competências para manter a função no futuro. Os resultados do estudo revelam que três em cada quatro Organizações (76%) têm vindo a investir em equipas dedicadas e com competências em Gestão da Continuidade do Negócio.

As competências em Gestão da Continuidade do Negócio foram maioritariamente adquiridas em conferências e congressos dedicados a este tema (68%), embora comece a ser já comum que os profissionais da Continuidade do Negócio (23%) frequentem cursos de formação nos requisitos da norma de certificação de Sistemas de Gestão da Continuidade do Negócio, ISO 22301, para implementar programas de Gestão da Continuidade do Negócio alinhados com as boas práticas.

Alguns profissionais da Continuidade do Negócio investem também em certificações profissionais, tais como ISO 22301 *Lead implementer* ou ISO 22301 *Lead Auditor* (13%) em especial em Organizações certificadas ou que pretendem certificar o seu Sistema de Gestão da Continuidade do Negócio neste referencial.

Gráfico 5: Competências das Equipas de Gestão da Continuidade do Negócio

Competências adquiridas através de…



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

Continuidade do Negócio

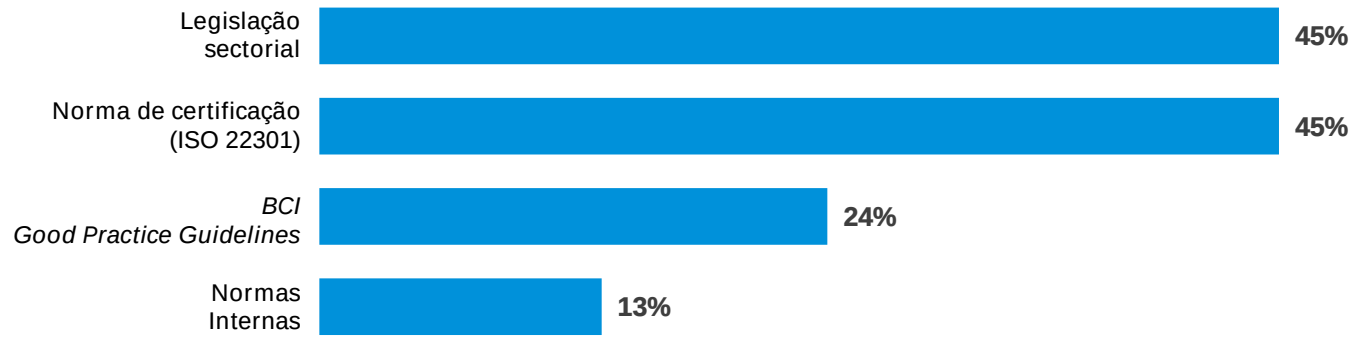
A decisão de implementar um programa de Gestão da Continuidade do Negócio implica procurar um modelo de referência que defina as boas práticas a seguir.

Quase metade das Organizações (45%) seguem as recomendações da legislação sectorial nesta matéria. No sector financeiro existem recomendações dos órgãos de supervisão para a implementação de um programa de Gestão da Continuidade do Negócio. Nos sectores de Telecomunicações, Energia e Transportes, existem directivas comunitárias relacionadas com a segurança e Continuidade dos Serviços, transpostas para Portugal.

De igual forma, quase metade das Organizações (45%) seguem os requisitos da norma de certificação de Sistemas de Gestão da Continuidade do Negócio, ISO 22301, como uma boa prática para a implementação de um programa de Gestão da Continuidade do Negócio independentemente de pretender, ou não, obter a certificação do Sistema de Gestão da Continuidade do Negócio implementado.

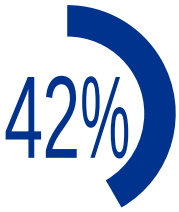
13% das Organizações, na sua maioria grandes multinacionais, seguem normas internas e modelos corporativos para a Gestão da Continuidade do Negócio.

Gráfico 6: Modelo de referência para Continuidade do Negócio



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

das Organizações **implementou** um **Sistema de Gestão da Continuidade do Negócio**



destas Organizações **certificou** ou pretende **certificar** o seu **Sistema de Gestão da Continuidade do Negócio**

> "Possuímos metodologias e práticas baseadas na norma ISO 22301, não estando formalizado um Sistema de Gestão da Continuidade do Negócio."

Pedro Cid
Director Geral
Auchan Portugal

Pedro Cid, Director Geral da Auchan Portugal, explica a abordagem da Auchan para a implementação da Gestão da Continuidade do Negócio: "Possuímos metodologias e práticas baseadas na norma ISO 22301, não estando formalizado um Sistema de Gestão da Continuidade do Negócio. As actividades relacionadas com a Continuidade do Negócio estão integradas em cada área, com a coordenação e supervisão da Direcção de *Performance*."

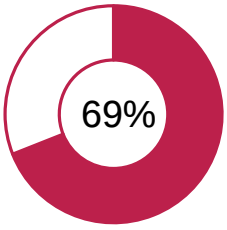
João Torres, CEO da EDP Distribuição, refere a relevância da certificação do Sistema de Gestão da Continuidade do Negócio para a Organização: "Desde que obtivemos a certificação, o Sistema de Gestão da Continuidade do Negócio é anualmente auditado. Um dos segredos essenciais é que toda a Organização sabe o que tem de fazer e da importância do seu contributo para manter a certificação."

Mário Vaz, CEO da Vodafone Portugal, afirma que a certificação está no horizonte: "Não temos à data de hoje um Sistema da Gestão da Continuidade do Negócio certificado, mas o programa de Gestão da Continuidade do Negócio estará seguramente alinhado com as exigências da certificação. É uma questão de prioridades, não estamos neste momento a trabalhar na certificação. Trabalharemos nela assim que terminarmos outros programas bastante relevantes, até para a Continuidade do Negócio."

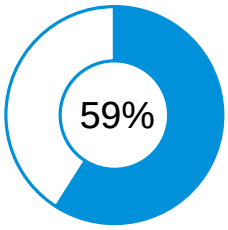
João Luis Baptista, COO da SIBS, explica a abordagem da sua empresa: "Para que a SIBS mantenha o patamar de resiliência e fiabilidade desejados, temos assegurado que o programa de Gestão da Continuidade do Negócio tem os recursos necessários, que a Política se encontra aprovada e alinhada com a estratégia da empresa, que o Plano de Exercícios aprovado está em implementação e que a sua execução é controlada e monitorizada através de indicadores e relatórios, e, por fim, que a equipa responsável está devidamente mandatada, por forma a implementar e manter uma Gestão da Continuidade do Negócio adequada às necessidades da empresa."

Gráfico 7: Estratégia da Continuidade do Negócio

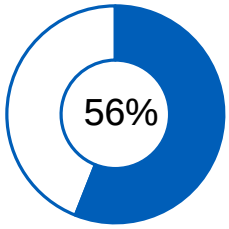
Percentagem de Organizações que realizam…



Análise de Impacto no Negócio às funções críticas do negócio

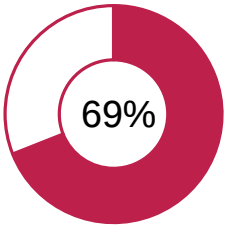


Avaliação do Risco aos recursos que suportam as funções críticas

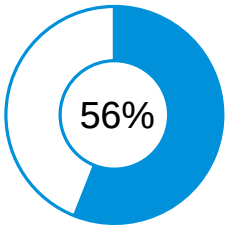


Ambas - Análise de Impacto no Negócio e Avaliação do Risco

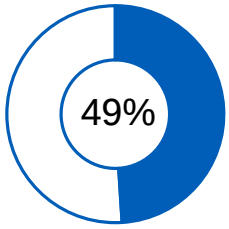
Percentagem de Organizações cuja Estratégia da Continuidade do negócio inclui…



Soluções de recuperação das funções críticas nos tempos definidos na Análise de Impacto no Negócio



Controlos preventivos para reduzir a exposição ao risco identificado na Avaliação do Risco



Ambas - Soluções de recuperação e controlos preventivos

Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

A implementação de um Sistema de Gestão da Continuidade do Negócio no referencial da norma ISO 22301 obriga à definição de uma Estratégia de Continuidade do Negócio baseada na realização de duas actividades essenciais: uma Análise do Impacto no Negócio e uma Avaliação do Risco.

A Análise do Impacto no Negócio tem como objectivo analisar, ao longo do tempo, o impacto da interrupção das funções críticas que suportam produtos e serviços chave da Organização e determinar as prioridades, e os recursos necessários, para assegurar a recuperação antes de o impacto (financeiro, reputacional ou legal) da indisponibilidade destas funções se tornar inaceitável.

A Avaliação do Risco tem como objectivo identificar eventos que possam comprometer a disponibilidade dos recursos que suportam as funções críticas (recursos humanos, instalações, Sistemas de Informação, fornecedores), analisar a probabilidade de ocorrência destes eventos e o impacto nas funções críticas caso ocorram, e identificar os eventos de risco que necessitam de tratamento para baixar o nível de risco a que a Organização está exposta.

A Estratégia da Continuidade do Negócio tem como objectivo definir soluções que permitam recuperar as funções críticas nos tempos definidos na Análise do Impacto no Negócio e definir controlos preventivos para reduzir a exposição da Organização ao risco identificado na Avaliação do Risco.

Os resultados do estudo indicam que a maioria das Organizações (69%) realiza Análises do Impacto no Negócio e define soluções de recuperação das funções críticas nos tempos definidos, 59% realiza avaliações do risco e 56% define controlos preventivos para reduzir a exposição ao risco. No entanto, apenas 56% das Organizações realizam Análises de Impacto no Negócio em conjunto com Avaliações do Risco e apenas 49% definem uma Estratégia da Continuidade do Negócio que inclui soluções de recuperação e controlos preventivos.

João Torres, CEO da EDP Distribuição, explica o processo na sua Organização: "A EDP Distribuição começou por identificar e avaliar uma série de cenários de risco que podem afectar os recursos fundamentais e constituir vertentes de falha de Continuidade do Negócio: as pessoas, as infra-estruturas físicas, as infra-estruturas tecnológicas e os fornecedores e prestadores de serviço. Através desta análise foi possível seleccionar as Estratégias de Continuidade do Negócio mais apropriadas, que possibilitam prevenir a interrupção das actividades prioritárias."

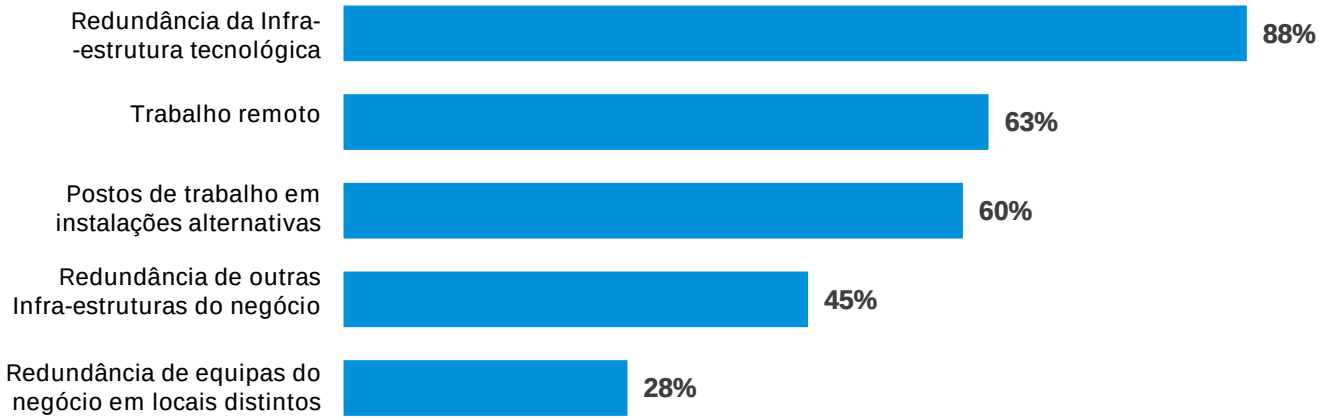
Após a aprovação da Estratégia da Continuidade do Negócio, o passo seguinte é garantir a implementação das soluções de recuperação do negócio definidas e dos controlos preventivos.

Os resultados do estudo indicam que as Organizações têm vindo a investir em soluções de recuperação do negócio. A maioria das Organizações (88%) dispõem de redundância da infra-estrutura tecnológica, 63% possuem soluções de trabalho remoto e 60% possuem postos de trabalho em instalações alternativas em caso de indisponibilidade das instalações principais. De salientar que 28% das Organizações possuem redundância de equipas em locais distintos, o que permite minimizar a necessidade de postos de trabalho em instalações alternativas.

Os planos da Continuidade do Negócio são ferramentas vitais para responder, de forma eficaz e eficiente, a incidentes disruptivos. Descrevem as actividades das várias equipas para responder à emergência, gerir a crise e recuperar as funções do negócio, usando as soluções de recuperação implementadas.

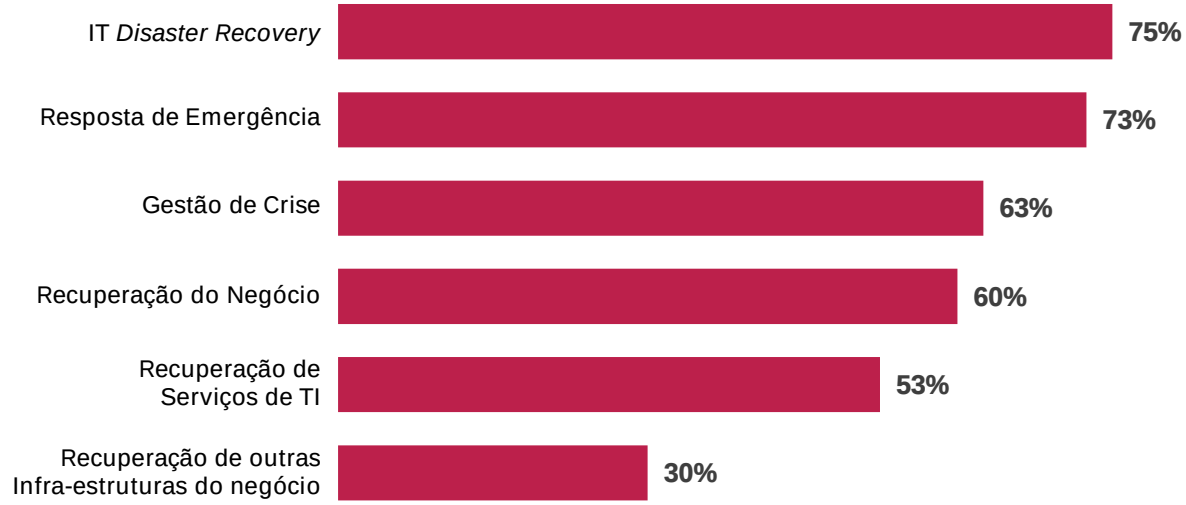
A maioria das Organizações (75%) possuem planos de IT *Disaster Recovery* e de Resposta de Emergência (73%) que tipicamente já existem antes da Organização iniciar a implementação da Gestão da Continuidade do Negócio. No entanto, mais de metade possuem também Planos de Gestão de Crise (63%), Planos de Recuperação do Negócio (60%) e Planos de Recuperação dos Serviços de TI (53%) típicos de um programa de Gestão da Continuidade do Negócio.

Gráfico 8: Soluções de Recuperação do Negócio



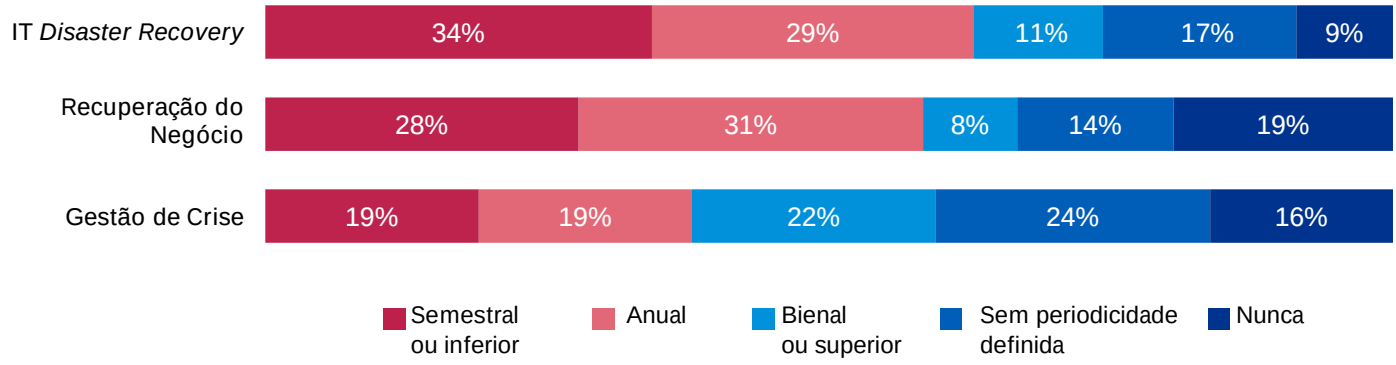
Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

Gráfico 9: Planos da Continuidade do Negócio



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

Gráfico 10: Exercícios e Testes



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

Após a operacionalização da Estratégia, é essencial avaliar a sua eficácia e eficiência através da realização de exercícios e testes envolvendo todas as áreas, de negócio e de suporte, com responsabilidades ao nível da Gestão da Continuidade do Negócio.

A grande maioria das Organizações (91%) realiza testes de IT *Disaster Recovery* e 63% realiza estes testes com periodicidade anual ou inferior. Estes resultados demonstram uma vez mais a importância vital das Tecnologias de Informação no suporte das operações de negócio e a preocupação das Organizações em assegurar uma recuperação rápida e eficaz da infra-estrutura tecnológica após um desastre.

81% das Organizações realiza também exercícios de Recuperação do Negócio e 59% realiza estes exercícios com periodicidade anual ou inferior, demonstrando a relevância de exercitar os papéis das equipas das áreas de negócio de forma a assegurar uma recuperação organizada e célere das funções críticas em instalações alternativas após um desastre.

Os exercícios de Gestão de Crise, que permitem exercitar os papéis da Administração e Gestão de Topo na gestão de uma crise decorrente de um incidente disruptivo, articulando o posicionamento da Organização com a comunicação social, invocando os planos da Continuidade do Negócio e accionando as equipas tácticas no terreno, são também realizados por 84% das Organizações inquiridas. Dada a sua natureza estratégica, este tipo de exercícios são realizados com uma periodicidade menor, apenas 38% das Organizações realiza estes exercícios com periodicidade anual ou inferior e 22% das Organizações realizam estes exercícios com frequência bienal ou superior.

Pedro Cid, Director Geral da Auchan Portugal, partilha a sua visão sobre os exercícios de Continuidade do Negócio na Auchan: "A Continuidade do Negócio é uma apólice de seguros que não queremos accionar, a não ser em exercícios. Temos uma sala de situação e várias células de gestão de crise e planos de contingência que accionamos em função da tipologia do incidente."

das Organizações realizaram **Exercícios integrados com equipas internas** (Gestão de Crise, Recuperação do Negócio, IT *Disaster Recovery*)

das Organizações realizaram **Exercícios integrados com equipas internas e externas** (fornecedores, reguladores, serviços de emergência)

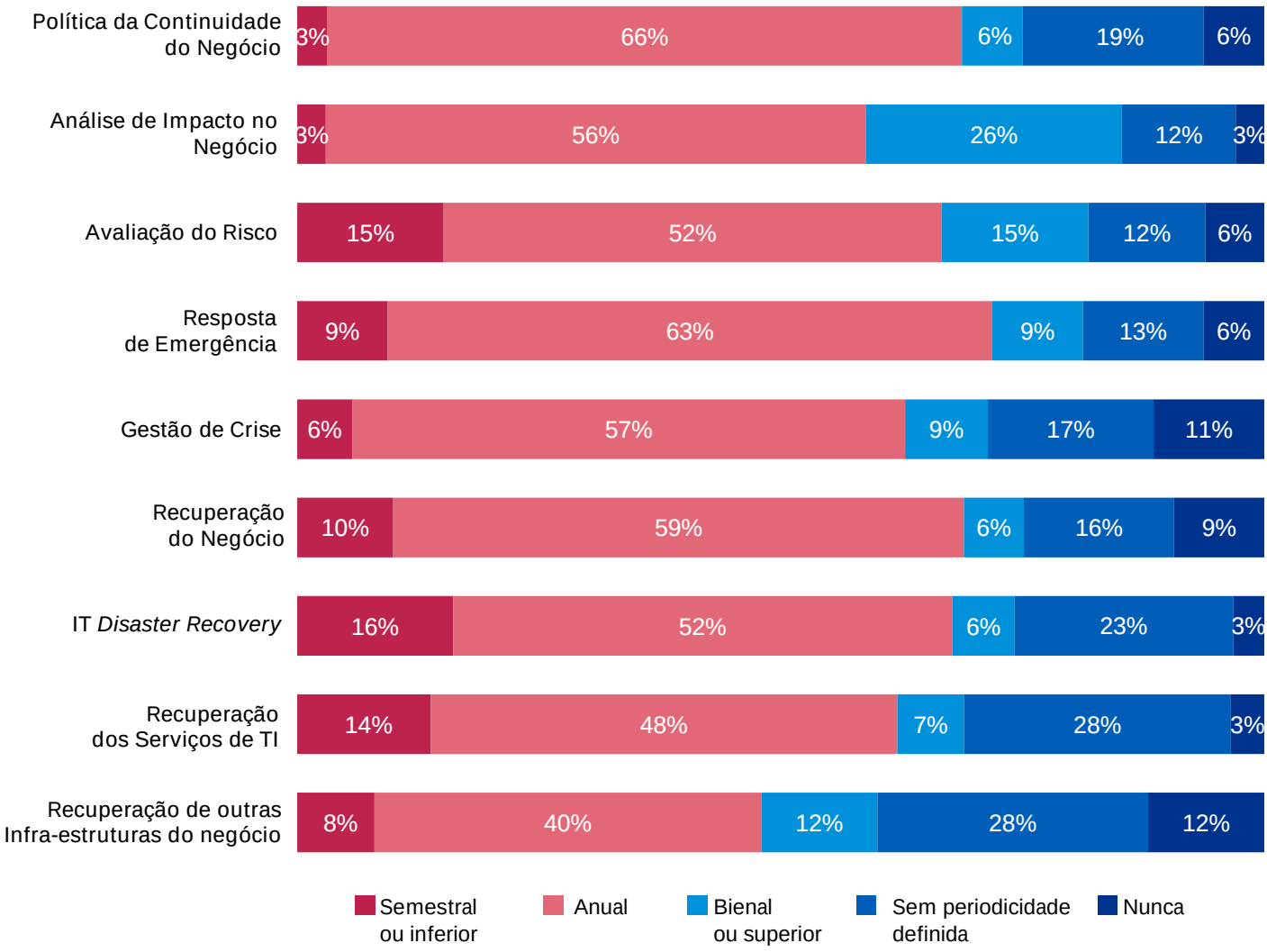
A implementação de um Sistema de Gestão da Continuidade do Negócio no referencial da norma ISO 22301 obriga à revisão periódica da documentação, de forma a assegurar que todos os documentos reflectem a realidade actual da Organização.

A documentação do SGCN deve ser revista pelo menos durante cada uma das fases de cada ciclo PDCA, que frequentemente tem uma periodicidade anual, e sempre que se justifique, nomeadamente, quando ocorrem mudanças estruturais na Organização.

Os resultados do estudo indicam que as Organizações realizam, de facto, uma revisão regular da documentação da Gestão da Continuidade do Negócio.

A generalidade dos documentos da Gestão da Continuidade do Negócio, desde a Política da Continuidade do Negócio até aos documentos de Recuperação do Negócio, IT *Disaster Recovery* e Continuidade dos Serviços de TI são revistos com periodicidade anual ou semestral por mais de metade das Organizações.

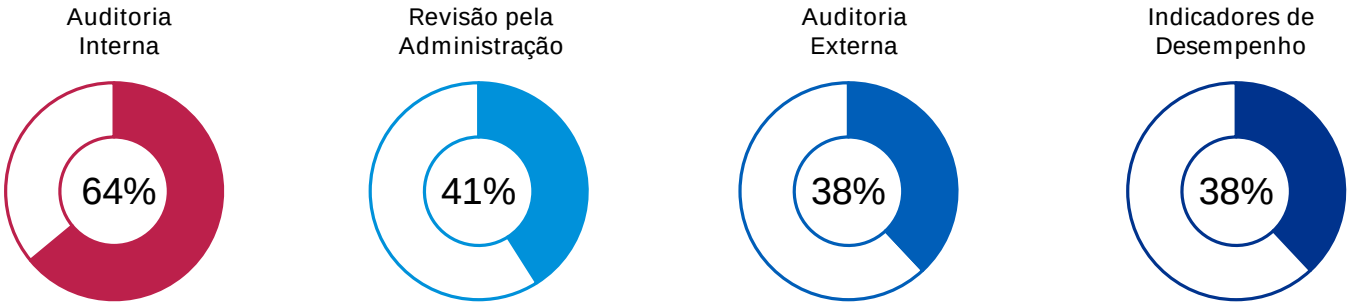
Gráfico 11: Periodicidade da Revisão da Documentação da GCN



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

Gráfico 12: Monitorização e Avaliação do Desempenho

O Programa de Gestão da Continuidade do Negócio é monitorizado e avaliado através de…



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

Após a implementação de um Sistema de Gestão da Continuidade do Negócio no referencial da norma ISO 22301, este entra em manutenção, em ciclos *Plan-Do-Check-Act* que asseguram a sua melhoria contínua (consultar página 6 para maior detalhe).

A fase de monitorização e avaliação do desempenho (*Check* no ciclo PDCA) pretende assegurar que:

- O SGCN cumpre os objectivos da política da Continuidade do Negócio, através da recolha e análise de indicadores de desempenho;
- O SGCN está em conformidade com os requisitos legais e regulamentares aplicáveis e normas internacionais de referência, recorrendo à realização de Auditorias, quer internas, quer externas; e
- O desempenho do SGCN é revisto pela Administração. Nesta revisão, são discutidos os resultados da avaliação do desempenho do programa que inclui a análise de indicadores de desempenho e das não conformidades resultantes de relatórios de Auditorias e de relatórios de Testes e Exercícios e são propostas acções de melhoria e acções correctivas.

O método de avaliação de desempenho dos programas da Gestão da Continuidade do Negócio mais comum é a Auditoria Interna, 64% das Organizações incluíram a função da Gestão da Continuidade do Negócio nos seus programas de auditoria interna.

No entanto, apenas 38% das Organizações monitorizam o programa da Gestão da Continuidade do Negócio através de indicadores de desempenho e 41% analisam regularmente o desempenho do programa da Gestão da Continuidade do Negócio e aprovam um plano de acção para melhorar o desempenho através de revisões pela Administração, o que permite concluir que existe ainda um caminho a percorrer pelas Organizações na implementação de mecanismos de avaliação de desempenho e melhoria contínua dos seus programas da Gestão da Continuidade do Negócio.

João Luis Baptista, COO da SIBS, descreve o processo de avaliação de desempenho do programa da Gestão da Continuidade do Negócio da SIBS, "São registados e analisados vários indicadores e produzidos relatórios que permitem validar a eficácia do programa. Estes relatórios abrangem os vários testes e exercícios efectuados, de forma habitual ao longo do ano, para analisar os índices de resiliência dos serviços e das equipas envolvidas face à estratégia de negócio da empresa. Adicionalmente, é analisado o relatório de auditorias internas que são efectuadas ao longo do ano."

Mário Vaz, CEO da Vodafone Portugal, retrata também a realidade da Vodafone: "Faço um acompanhamento permanente dos KPI's dos diferentes serviços que consideramos críticos e uma revisão regular do programa da Gestão da Continuidade do Negócio com a equipa, em que se discute as alterações pretendidas e as adaptações à realidade necessárias. Nesta reunião de acompanhamento faz-se

também o seguimento das acções correctivas e de melhoria planeadas em reuniões anteriores." E acrescenta, "Esta função é também auditada regularmente pela equipa de Auditoria Interna."

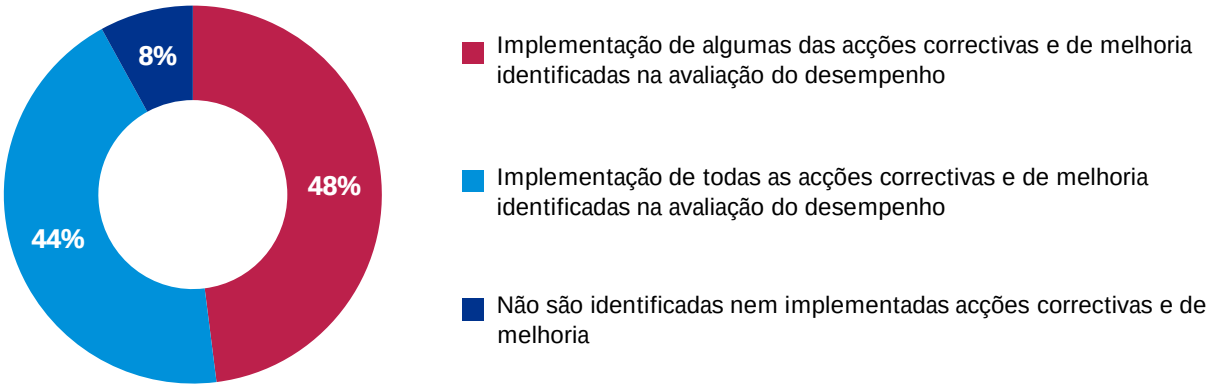
A fase de melhoria contínua (*Act* no ciclo PDCA) tem como objectivo identificar oportunidades de melhoria, analisar as causas das não conformidades encontradas na fase de avaliação do desempenho e implementar as acções correctivas e preventivas necessárias para eliminar as não conformidades bem como oportunidades de melhoria que tenham sido identificadas, melhorando assim o desempenho do SGCN em cada ciclo.

João Torres, CEO da EDP Distribuição, descreve o processo de avaliação de desempenho e melhoria contínua do Sistema de Gestão da Continuidade do Negócio da EDP Distribuição: "O PCA preside o Comité de Continuidade do Negócio onde se encontram formalmente definidas as Unidades Organizativas da Empresa com as responsabilidades e atribuições ao nível da Gestão da Continuidade do Negócio e mais directamente relacionadas com a gestão dos serviços críticos da Empresa. O Comité reúne anualmente, no qual se apresentam as iniciativas mais relevantes, os resultados alcançados, revisitando os indicadores de desempenho do SGCN. São também identificadas e aprovadas as principais acções de mitigação do risco, para implementação e acompanhamento no ciclo seguinte e, sempre que necessário, inclui a reavaliação da adequação do âmbito, da política e dos objectivos de Continuidade do Negócio. Deste modo a Gestão de Topo garante o envolvimento transversal e o comprometimento da Organização com a Continuidade do Negócio." E acrescenta: "O suporte da Revisão pela Gestão inclui também o Subcomité de Continuidade do Negócio, que reúne periodicamente três vezes por ano. Estas reuniões permitem garantir a manutenção e a melhoria contínua do Sistema de Gestão de Continuidade do Negócio, alinhada com os objectivos estabelecidos. Revisitam-se todas as acções em curso para partilha do ponto de situação e próximos passos."

Pedro Cid, Director Geral da Auchan Portugal, partilha uma realidade semelhante: "As acções relativas à Continuidade do Negócio aprovadas no Comité de Segurança são incluídas no nosso sistema de *Balanced Scorecard* corporativo e são acompanhadas em reuniões de ponto de situação mensais. Adicionalmente, as áreas com responsabilidades ao nível da Continuidade do Negócio incluem estas acções nos seus objectivos semestrais e são também avaliadas pela concretização destes seus objectivos." E acrescenta: "Temos também a auditoria interna corporativa e uma equipa de auditoria interna local, que audita tudo incluindo as práticas de Continuidade do Negócio e auditorias externas, por exemplo, das companhias de seguros. Estas auditorias, descrevem a nossa realidade como estando alinhados com aquilo que é um Programa de Gestão da Continuidade do Negócio."

Gráfico 13: Melhoria Contínua

As Organizações asseguram a melhoria contínua do Programa de Gestão da Continuidade do Negócio através da…



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

Continuidade dos Serviços de TI

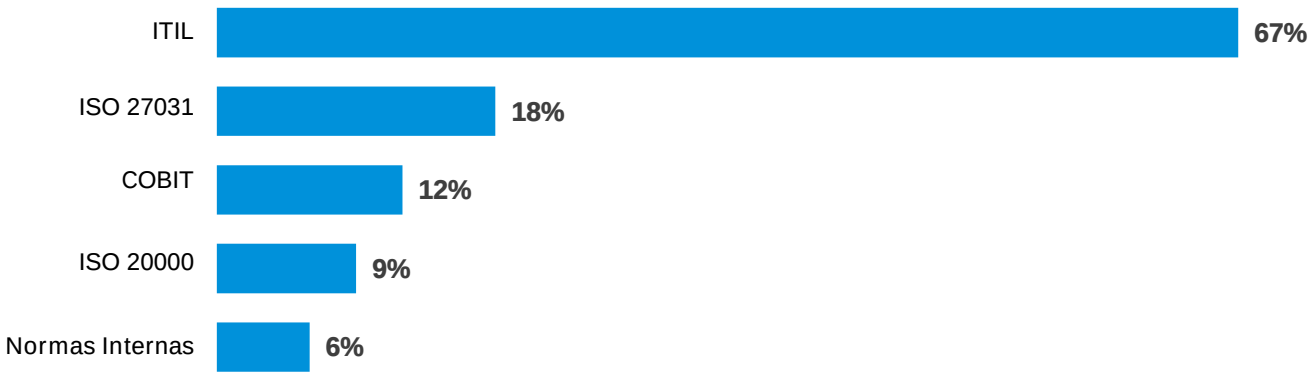
As Organizações têm vindo a apostar na transformação digital dos seus modelos de negócio de modo a assegurar o foco nas expectativas dos seus clientes e ganhos de eficiência nas suas operações, através da inovação tecnológica.

Os novos modelos de negócio, disponibilizam frequentemente serviços ao cliente através de vários canais que exigem plataformas com disponibilidade de 24 horas, 7 dias por semana, 365 dias por ano e a indisponibilidade da plataforma tem um impacto imediato na satisfação do cliente e na reputação da Organização. Por outro lado, os Sistemas de Informação são hoje vitais para as operações em qualquer ramo de actividade e a sua indisponibilidade tem um impacto imediato na eficiência operacional.

A Continuidade dos Serviços de TI tem como objectivo manter as funções críticas do negócio através da prevenção, detecção, resposta e recuperação de incidentes disruptivos que possam afectar o normal funcionamento das TI.

A maioria das Organizações (67%) segue o modelo de referência ITIL para implementar a Continuidade de Serviços de TI, 18% seguem a norma ISO 27031 que faz parte do grupo de normas ISO 27000 relacionadas com a segurança de informação e 12% seguem o modelo COBIT que é um *framework* que estabelece objectivos de controlo para as Tecnologias de Informação, usado frequentemente na implementação de sistemas de controlo interno.

Gráfico 14: Modelo de referência para Continuidade dos Serviços de TI



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

> “Desde o primeiro dia, a SIBS tem realizado diversos investimentos na resiliência e fiabilidade dos seus serviços, que apresentam um nível de *uptime* na ordem dos 99,9%.”

João Luis Baptista
COO
SIBS

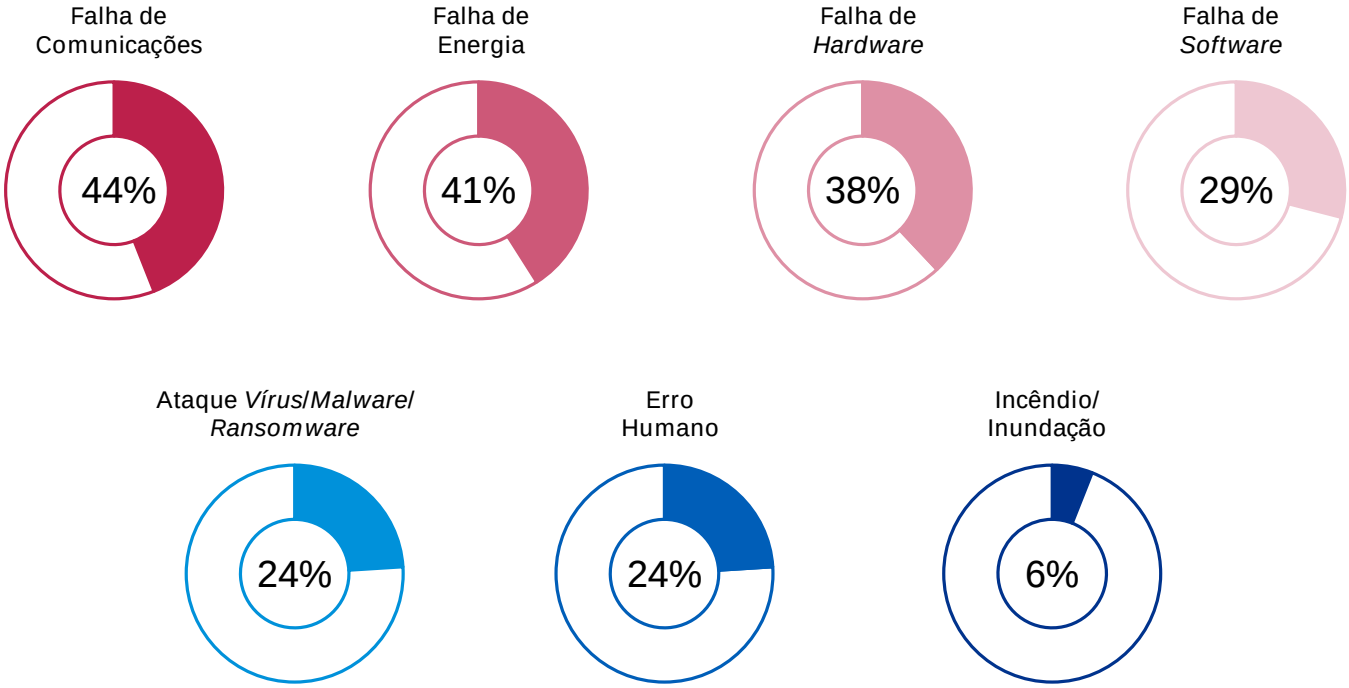
João Luis Baptista, COO da SIBS, descreve o projecto de transformação da SIBS através da nova plataforma ARCTIC: “Os desafios que a SIBS assumiu para o futuro, e as necessidades dos negócios nacional e internacional, seja em termos de *time-to-market*, como de oferta de serviços individualizados, levou à necessidade de desenvolvimento de uma nova plataforma tecnológica. Um programa que transforma o Sistema de Informação da SIBS, que altera a abordagem na concepção de produtos de negócio e a visão do negócio, orientada a serviços. Surgiu assim o ARCTIC, (*Availability, Resilence, Cost Reduction, Time-to-Market, Improvement of IT Systems Capabilities and Flexibility and Compliance*).” E acrescenta os mecanismos de resiliência e mitigação de risco implementados: ”A mitigação da esmagadora maioria dos riscos e a prestação dos serviços com o nível de disponibilidade referidos assenta num modo de Alta-Disponibilidade, com redundâncias, e num regime multi--vendor. Adicionalmente, os controlos e mecanismos de segurança implementados que seguem as melhores práticas internacionais da área (PCI-DSS), permitem fornecer os serviços de forma segura e mitigar os riscos de segurança.

Os serviços da SIBS já suportados pelo ARCTIC beneficiam de um nível de resiliência acrescida já que esta plataforma funciona num regime de processamento distribuído por dois *Data Centres* (Activo-Activo). Em caso de incidente grave num dos *Data Centre*, os fluxos transaccionais do centro afectado são direccionados, automaticamente, para o outro *Data Centre*, o qual tem capacidade instalada para suportar a carga transaccional de toda a Rede SIBS. Para os serviços ainda não incluídos no ARCTIC, e na eventualidade de eventos catastróficos/disruptivos que impeçam esta disponibilidade dos serviços, a SIBS dispõe de um *Data Centre* alternativo com capacidade de assegurar todos os serviços prestados neste centro, com o mesmo nível de disponibilidade, qualidade e segurança.”

João Luis Baptista, finaliza “As soluções de Continuidade implementadas são desenhadas com o objectivo de recuperar totalmente os serviços, sem perda, ou com a menor perda de dados e da forma mais célere. As soluções são testadas e melhoradas através de exercícios regulares em três ambientes, por forma a garantir a sua eficácia e eficiência.”

Gráfico 15: Incidentes disruptivos

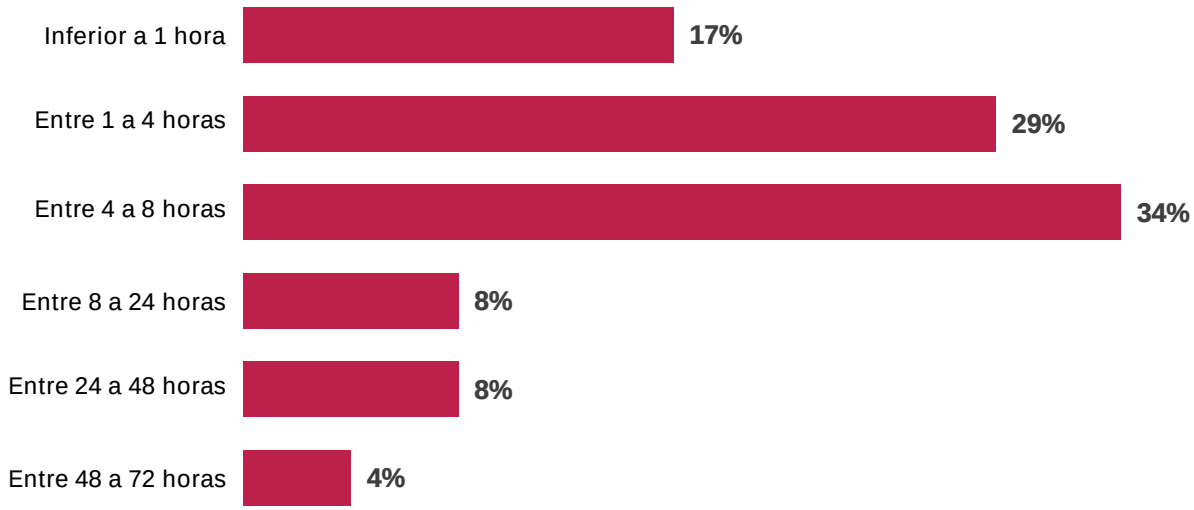
Incidentes disruptivos que levaram a indisponibilidade dos serviços de TI nos últimos cinco anos…



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

Gráfico 16: Tempo máximo de indisponibilidade dos Serviços de TI

Tempo máximo de indisponibilidade devido a incidentes disruptivos nos últimos cinco anos…



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

O estudo revela que 71% das Organizações sofreram um incidente disruptivo que causou a indisponibilidade dos Serviços de TI nos últimos cinco anos.

Estes incidentes encontram-se relacionados sobretudo com as falhas de comunicações (44%), falhas de energia (41%), mas também falhas de *hardware* (38%), falhas de *software* (29%) e Ataque Vírus/*Malware*/*Ransomware* (24%).

Os incidentes de segurança informática têm vindo a aumentar e são alvo de forte cobertura mediática, estando actualmente nas agendas das administrações.

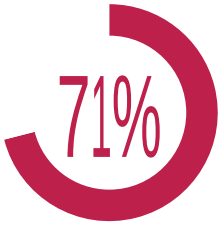
João Torres, CEO da EDP Distribuição, partilha a sua preocupação com o risco de entrada maliciosa dos sistemas críticos da EDP Distribuição: "Grande parte da nossa actividade está suportada em Sistemas de Informação. O tema da Cibersegurança é um dos temas que mais nos preocupa e tem vindo a subir nas prioridades. É uma área que exige soluções robustas e um forte investimento. A EDP possui duas áreas de sistemas, os sistemas operacionais do negócio (SCADA), que controlam as redes de distribuição de electricidade, e os sistemas comerciais, que asseguram a gestão de clientes e a facturação. Quando houve o recente ataque informático (*WannaCry*) a minha preocupação foi principalmente com os sistemas SCADA, sem *email* ainda conseguimos trabalhar, sem os sistemas SCADA não." E acrescenta os mecanismos implementados para assegurar a resiliência: "Para os sistemas operacionais SCADA, que são críticos, foi implementada redundância, conseguimos operar toda a rede a partir de Lisboa ou do Porto, o que nos permite ter segurança do ponto de vista da Continuidade do Negócio. Na vertente dos sistemas comerciais, que é uma actividade gerida em termos corporativos pela EDP, sei que os temas da Cibersegurança e da Continuidade do Negócio estão endereçados."

Pedro Cid, Director Geral da Auchan, destaca igualmente o recente episódio do *WannaCry:* "Ocorreu uma situação de ciberataque, mas felizmente graças às nossas equipas e aos nossos mecanismos de protecção de sistemas informáticos, não nos afectou."

Mário Vaz, CEO da Vodafone Portugal, está também preocupado com temas de Cibersegurança: "No mundo digital em que hoje vivemos estamos essencialmente preocupados com a entrada maliciosa nos nossos sistemas e com o acesso não autorizado a dados pessoais." E refere os investimentos realizados recentemente em redundância da infra-estrutura tecnológica: "Nos últimos dois ciclos orçamentais investimos milhões de Euros para garantir a resiliência da infra-estrutura de rede na tecnologia 4G, que era a componente que faltava assegurar, o que consistiu num investimento significativo".

Os resultados indicam que das Organizações que sofreram um incidente disruptivo nos últimos cinco anos, 54% ficaram com os Serviços de TI indisponíveis por mais de 4 horas, 34% de 4 a 8 horas, 8% entre 8 e 24 horas, 8% entre 24 e 48 horas e 4% entre 48 e 72 horas.

João Luis Baptista, COO da SIBS, revela o impacto da indisponibilidade da plataforma da SIBS para a qual "qualquer falha, por pequena que seja, teria impactos sérios na economia nacional. Além dos potenciais impactos externos, qualquer disrupção nos serviços teria um impacto financeiro na actividade da SIBS, proporcional ao tempo de interrupção, uma vez que uma parte relevante dos modelos de negócio da SIBS assenta sobre a actividade transaccional unitária." E acrescenta, "Os serviços da SIBS, que incluem operações *Core* da actividade da rede MULTIBANCO como os levantamentos em caixas e compras nos terminais de pagamentos automáticos, são processados em dois centros distintos, distribuindo-se a carga transaccional pelas duas instâncias."

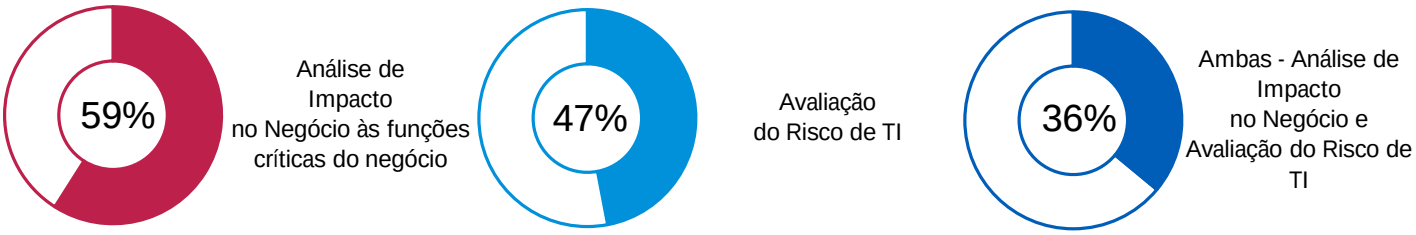


das Organizações sofreram um incidente disruptivo que causou a indisponibilidade dos Serviços de TI

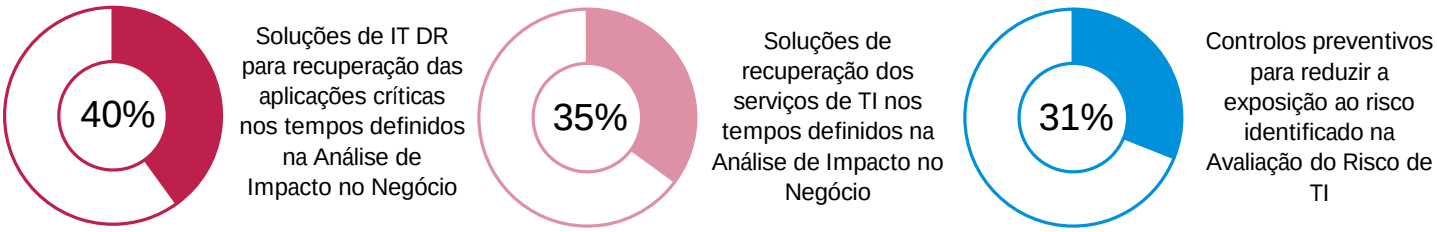
destas Organizações ficaram com os Serviços de TI indisponíveis por mais de quatro horas

Gráfico 17: Estratégia da Continuidade dos Serviços de TI

Percentagem de Organizações que realizam…



Percentagem destas Organizações cuja Estratégia da Continuidade dos Serviços de TI inclui…



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

A Estratégia da Continuidade dos Serviços de TI deve ser baseada na realização de duas actividades essenciais: uma Análise de Impacto no Negócio e uma Avaliação do Risco de TI.

A Análise de Impacto no Negócio tem como objectivo analisar, ao longo do tempo, o impacto da interrupção das funções críticas do negócio e dos Serviços de TI, identificando os seus tempos de recuperação e os seus requisitos de recuperação. A Análise de Impacto no Negócio das funções críticas pode ser realizada por outro Departamento que lidere a implementação da Gestão da Continuidade do Negócio na Organização.

Mais de metade das Organizações (59%) realizaram uma Análise de Impacto no Negócio, das quais 55% foram realizadas pelo Departamento de TI.

A Avaliação do Risco de TI tem como objectivo avaliar os eventos de risco que possam comprometer a entrega dos Serviços de TI. Esta avaliação pode também ser feita por outro Departamento, por exemplo, pelo Departamento de Gestão do Risco.

47% das Organizações realizaram uma Avaliação do Risco de TI, das quais 88% foram realizadas pelo Departamento de TI.

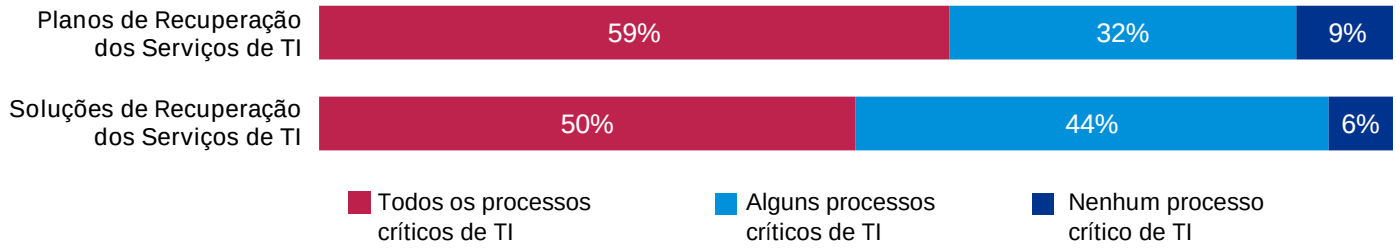
A Estratégia de Continuidade dos Serviços de TI tem como objectivo definir soluções de IT DR para recuperar as aplicações que suportam as funções críticas de negócio e soluções que permitam recuperar os Serviços de TI nos tempos definidos na Análise de Impacto no Negócio e definir controlos preventivos para reduzir a exposição da Organização ao risco identificado na Avaliação do Risco de TI.

40% das Organizações incluíram na Estratégia de Continuidade dos Serviços de TI, soluções de IT DR para recuperação de aplicações críticas e 35% incluíram soluções para recuperação dos Serviços de TI, com base nos tempos definidos na Análise de Impacto no Negócio.

31% das Organizações incluíram na Estratégia de Continuidade dos Serviços de TI controlos preventivos para reduzir a sua exposição ao risco identificado na Avaliação do Risco de TI.

Adicionalmente, apenas 26% das Organizações respondeu possuir uma Estratégia de Continuidade dos Serviços de TI alinhada e integrada com a Estratégia da Continuidade do Negócio, sendo claramente um aspecto a melhorar pelas Organizações para assegurar a resiliência dos Sistemas de Informação que suportam as funções críticas.

Gráfico 18: Planos e Soluções de Recuperação dos Serviços de TI



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

Os Planos e Soluções de Recuperação dos Serviços de TI são ferramentas essenciais para gerir e responder, de forma eficaz e eficiente, a eventos disruptivos que impactem os Serviços de TI.

Os Planos de Recuperação dos Serviços de TI descrevem as actividades dos técnicos de TI para garantir a recuperação dos Serviços de TI.

91% das Organizações definiram Planos de Recuperação dos Serviços de TI e 59% definiram planos para todos os processos críticos de TI.

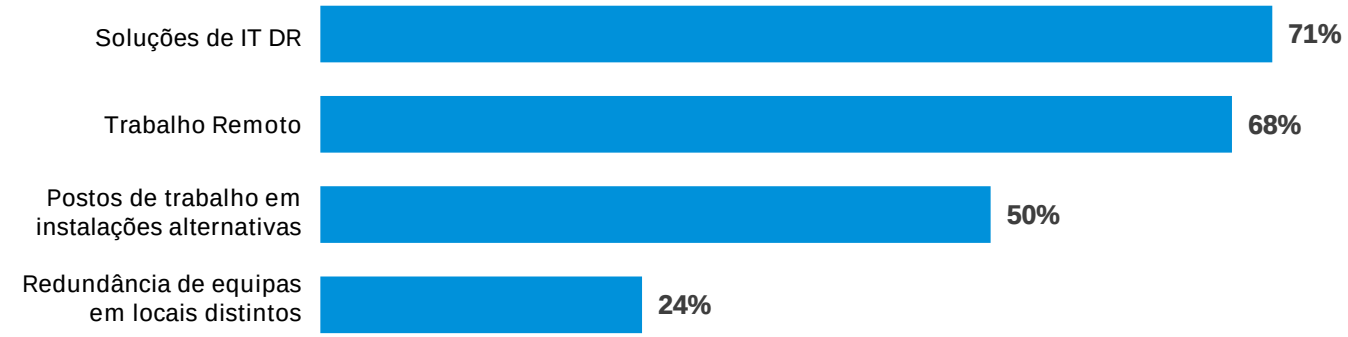
As soluções de Recuperação dos Serviços de TI permitem assegurar os processos críticos de TI em caso de indisponibilidade de aplicações de suporte a estes processos, indisponibilidade de técnicos de TI e/ou indisponibilidade de postos de trabalho.

A maioria das Organizações (71%) dispõem de Soluções de IT *Disaster Recovery* para recuperar aplicações críticas de suporte aos serviços de TI (e.g *service desk*, monitorização).

Duas em cada três Organizações (68%) dispõem de soluções de trabalho remoto (PC, dispositivos de autenticação para acesso remoto) para a recuperação dos Serviços de TI em caso de indisponibilidade de postos de trabalho. Uma vez que a solução de trabalho remoto nem sempre permite a recuperação total dos serviços, por questões tecnológicas ou operacionais, 50% das Organizações optam pela implementação de postos de trabalho preparados em instalações alternativas (próprias ou alugadas).

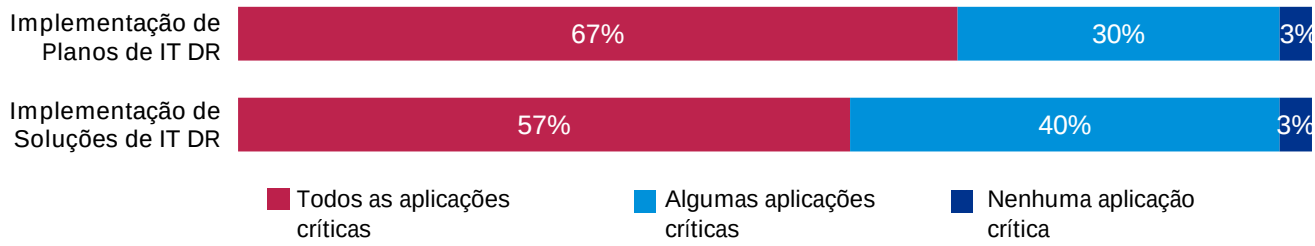
Finalmente, 24% dispõem de redundância de equipa em locais distintos que assegura a Continuidade dos Serviços de TI, embora com degradação do nível de serviço.

Gráfico 19: Soluções de Recuperação dos Serviços de TI



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

Gráfico 20: Planos e Soluções de IT *Disaster Recovery*



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

Os Planos e Soluções de IT DR visam responder, de forma eficaz e eficiente, a eventos disruptivos que impactem a infra-estrutura tecnológica que suporta as aplicações críticas para o negócio.

97% das Organizações definiram planos e implementaram soluções de IT DR, 67% definiram planos e 57% implementaram soluções de IT DR para todas as aplicações críticas.

As Organizações podem assegurar a continuidade operacional das suas aplicações críticas através de redundância da infra-estrutura tecnológica no *Data Centre* de Produção e num *Data Centre* Alternativo a uma distância razoável do *Data Centre* de Produção e recorrer a soluções *Cloud*.

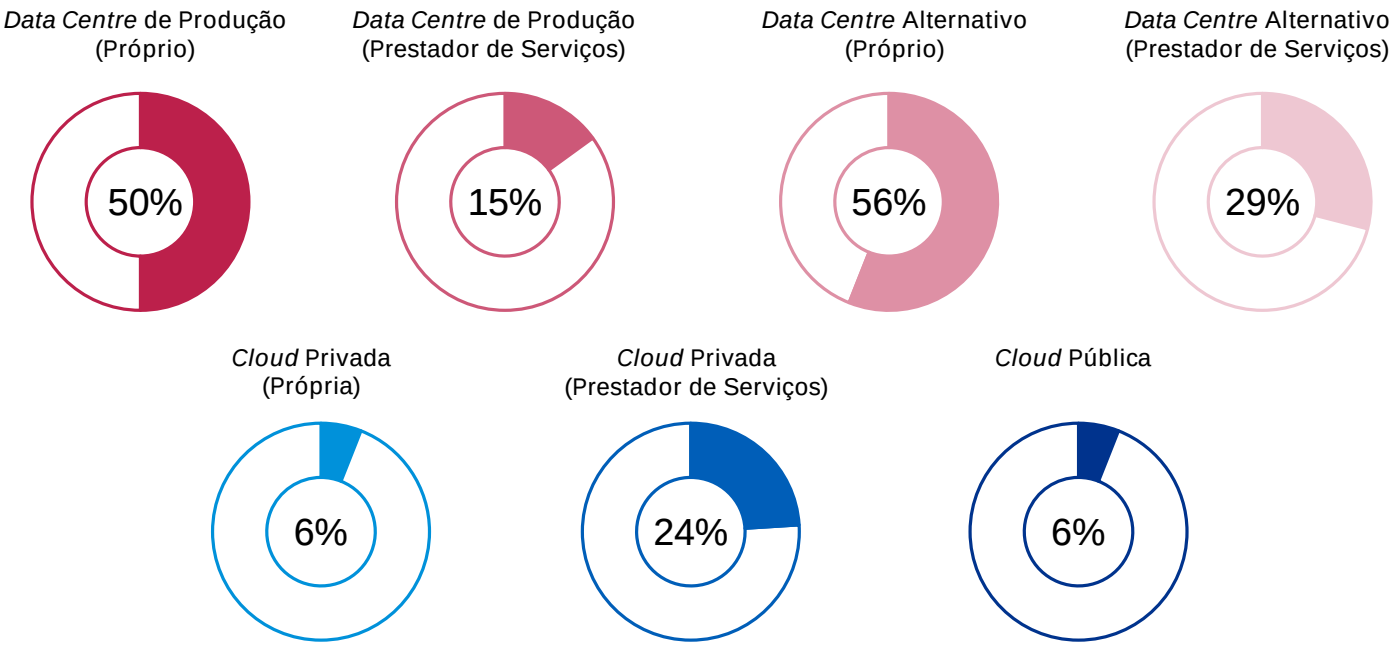
A maioria das Organizações possuem soluções de IT DR em *Data Centres* próprios, 50% possuem soluções no *Data Centre* de Produção e 56% soluções em *Data Centre* Alternativo.

Algumas Organizações optaram por soluções em *Data Centres* de prestadores de serviços, 15% possuem soluções no *Data Centre* de Produção e 29% soluções em *Data Centre* Alternativo.

As soluções de IT DR na *Cloud* têm vindo a aumentar, 24% das Organizações recorrem a soluções *Cloud* Privada num prestador de serviços e 6% recorrem a *Cloud* Pública.

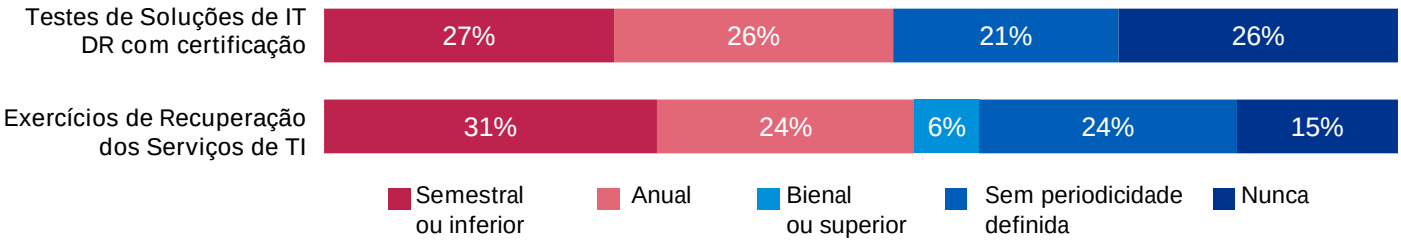
59% das Organizações implementaram várias soluções de IT DR em simultâneo, para recuperar sistemas diferentes.

Gráfico 21: Soluções de IT *Disaster Recovery*



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

Gráfico 22: Periodicidade de Exercícios e Testes de Continuidade dos Serviços de TI



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

Após a operacionalização da Estratégia de Continuidade dos Serviços de TI, é essencial avaliar a sua eficácia e eficiência através da realização de exercícios de recuperação dos Serviços de TI envolvendo as áreas técnicas e testes de IT DR envolvendo as áreas técnicas e os utilizadores do negócio para certificação funcional das aplicações em ambiente de IT *Disaster Recovery*.

A grande maioria das Organizações (74%) realiza testes às soluções de IT DR com certificação dos utilizadores, 53% com periodicidade anual ou inferior.

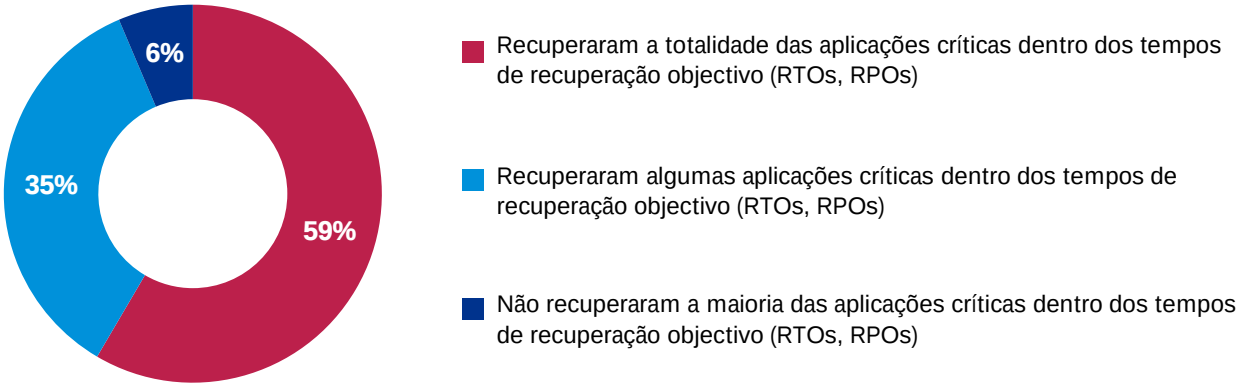
Os resultados do estudo revelam também que 85% das Organizações realizam exercícios de Recuperação dos Serviços de TI, 55% com frequência anual ou inferior.

Mais de metade das Organizações (59%) que realizaram testes de IT DR recuperaram a totalidade das aplicações críticas dentro dos tempos de recuperação objectivo (RTOs, RPOs) definidos na análise de impacto no negócio.

João Torres, CEO da EDP Distribuição, partilha como são realizados os testes de IT Disaster Recovery na EDP: "Anualmente são realizados dois ensaios globais de *Disaster Recovery* que envolvem testes de infra-estrutura e testes aplicacionais. Os testes de Infra-estrutura visam validar os procedimentos técnicos de recuperação, a operacionalidade da infra-estrutura de IT *Disaster Recovery* e o cumprimento de RTO e RPO na recuperação de cada aplicação/plataforma. Os testes aplicacionais visam verificar a operacionalidade das aplicações, após a recuperação da infra-estrutura, as interfaces aplicacionais e processos *batch* e a possibilidade de realização de processos de negócio críticos envolvendo várias aplicações. Finalmente, os testes de IT *Disaster Recovery* visam ainda familiarizar os utilizadores chave que asseguram a certificação funcional com as actividades a desempenhar no caso da activação real do Plano de IT *Disaster Recovery* e possibilitar a identificação de acções preventivas e correctivas para melhoria técnica e processual do Serviço, Plano de IT *Disaster Recovery* e Solução de IT Disaster Recovery da EDP."

Gráfico 23: Teste às soluções de IT *Disaster Recovery*

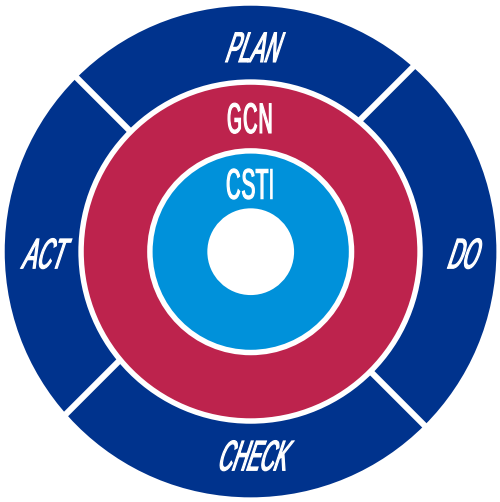
As Organizações que efectuaram Testes às soluções de IT *Disaster Recovery*…



Fonte: Estudo da Continuidade do Negócio, KPMG em Portugal

Serviços KPMG

A KPMG tem vindo a apoiar, desde 2006, grandes Grupos Económicos na implementação e auditoria de Sistemas de Gestão da Continuidade do Negócio (SGCN), incluindo as componentes de Gestão da Continuidade do Negócio (GCN) e Continuidade dos Serviços de TI (CSTI).



Os nossos profissionais têm dedicação exclusiva a projectos de Continuidade do Negócio, possuem até 10 anos de experiência e são certificados em normas internacionais de SGCN, nomeadamente, PECB *Certified* ISO 22301 *Lead Implementer/Auditor* e são reconhecidos através de prémios de prestígio a nível internacional, como *Business Continuity Consultant of the Year*, pela CIR *Awards*.

Os nossos serviços estão alinhados com as principais normas ISO de referência (i.e. ISO 22301, ISO 31000, ISO 27031) e abrangem todas as fases do ciclo PDCA:

PLAN:
- Sessões de formação ISO 22301 *Lead Implementer*
- Planear e acompanhar o SGCN (PMO)
- Definir a Política da CN/Política de CSTI
- Definir a estrutura de governo do SGCN/CN/CSTI
- Definir o Manual e Processos do SGCN
- Definir o Plano de Comunicação para o SGCN
- Definir e entregar iniciativas de comunicação e *awareness*

DO:
- Realizar Análise do Impacto no Negócio
- Realizar Avaliação do Risco
- Definir Estratégias de CN/ CSTI
- Definir Planos de Procedimentos de CN/CSTI
- Exercícios e Testes de Resposta de Emergência, Gestão de Crise, Recuperação do Negócio, IT *Disaster Recovery*, Continuidade dos Serviços de TI e Cibersegurança

CHECK:
- Sessões de formação à Auditoria Interna
- Auditorias de Conformidade ao SGCN e à Continuidade dos Serviços de TI
- Definir e monitorar Indicadores de desempenho do SGCN
- Definir e facilitar a Revisão pela Gestão

ACT:
- Definir Plano de Manutenção do SGCN
- Planear e acompanhar a implementação das iniciativas com vista a endereçar não conformidades e acções correctivas

A KPMG possui uma linha de serviços de Red Team que tem como objectivo simular um conjunto alargado de ataques desenhados para avaliar a resiliência das Pessoas, Redes, Sistemas, Aplicações e Instalações a um ataque de um adversário real altamente sofisticado, por exemplo, uma Organização de crime organizado ou um Estado.

Os testes Red Team são adaptados ao modelo de negócio de cada Organização e utilizam vectores de ataque sofisticados tais como phishing, malware e engenharia social através de actividades de war gaming simuladas num framework de testes controlado.

O framework de testes Red Team possui várias valências:

- Permite testar a eficácia da análise forense digital e da resposta a incidentes de Cibersegurança da Organização;
- Permite testar a resiliência e a capacidade defensiva da Organização a ataques;
- Disponibiliza indicadores de comprometimento que permitem criar alertas de ataques, adaptados a cada Organização;
- Permite analisar a exposição da Organização ao risco de recolha de informação com base na sua pegada digital, utilizando tecnologias *Open Source Intelligence* (OSINT);
- Ajuda a Organização a preparar os seus Sistemas para que eles resistam melhor a ataques;
- Cria cenários práticos e realistas para preparar a equipa de Ciberdefesa a responder a ataques;
- Simula ameaças reais e permite melhorar os sistemas de Detecção/Prevenção de Intrusões (IDS/IPS) e sistemas de Segurança de Informação & Gestão de Eventos (SIEM);
- Identifica vectores de ataque que seriam utilizados por criminosos para exfiltrar informações confidenciais ou segredos corporativos da Organização; e
- Qualifica a eficácia do programa de consciencialização de Cibersegurança da Organização.

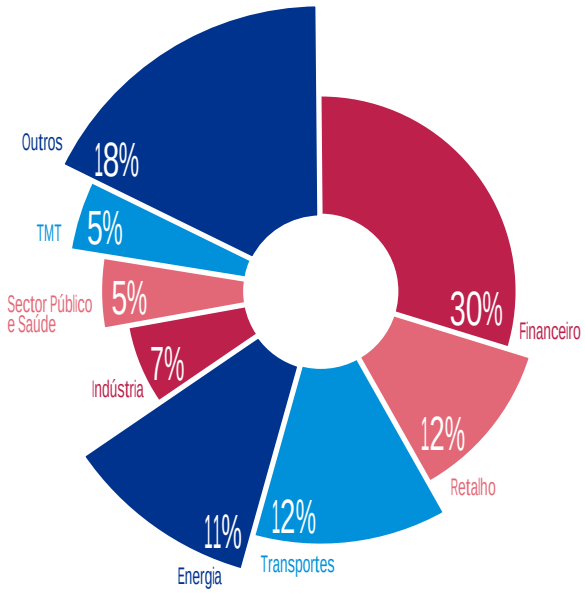
Os serviços Red Team da KPMG permitem identificar ameaças potenciais e o seu impacto nos processos de negócio da Organização e identificar e priorizar oportunidades de melhoria nos seus mecanismos de defesa actuais.

Os testes Red Team permitem avaliar a resiliência da Organização a Ameaças Persistentes Avançadas (APTs) usando as Tácticas, Técnicas e Procedimentos (TTPs) dos adversários.

Os serviços Red Team vão para além de Testes de Penetração que visam apenas identificar e validar vulnerabilidades em Redes, Sistemas e Aplicações, através de testes de âmbito mais restrito, de menor profundidade e realizados num curto espaço de tempo.

Serviços	Testes de Penetração	Red Team
Análise de vulnerabilidades	ü	ü
Scripts personalizados e inteligência aplicada	ü	ü
Simulação de ameaças internas	ü	ü
Engenharia social	-	ü
Simulação de adversários	-	ü
Intrusão via terceiros	-	ü
Técnicas avançadas de OSINT	-	ü
Ataques a dispositivos IoT	-	ü
Ataques *Wireless*, GSM, NFC, BLE e SDR	-	ü
Ataques a serviços de gestão de identidades e acessos	-	ü
Ataques direccionados, ATP TTPs	-	ü
Testes a controlos físicos de Segurança	-	ü

Metodologia e Agradecimentos



Os dados publicados neste estudo são baseados em dois questionários electrónicos – Gestão da Continuidade do Negócio e Gestão da Continuidade de Serviços de Tecnologias de Informação – respondidos, entre Setembro e Novembro de 2017, por 76 gestores responsáveis por estas funções nas suas Organizações e em entrevistas com quatro Administradores executivos com o pelouro da Gestão da Continuidade do Negócio.

Os gestores da Continuidade do Negócio e da Continuidade dos Serviços de TI que participaram no estudo pertencem a Organizações de sete sectores chave para a economia: Financeiro, Retalho, Transportes, Energia, Indústria, Sector Público & Saúde e Telecomunicações, Media e Tecnologia (TMT). A análise dos resultados foi realizada pelos profissionais da equipa de *Business Continuity* da KPMG em Portugal.

A KPMG agradece a valiosa contribuição dos gestores que partilharam informação sobre os programas de Gestão da Continuidade do Negócio das suas Organizações e dos quatro Administradores executivos que amavelmente partilharam a sua experiência de liderança da Gestão da Continuidade do Negócio:

- Mário Vaz, CEO da Vodafone Portugal
- João Torres, CEO da EDP Distribuição
- Pedro Cid, Director Geral da Auchan Portugal
- João Luis Baptista, COO da SIBS

Contactos

Nasser Sattar
Head of Advisory
T: +351 212 487 308
E: nsattar@kpmg.com

Rui Gonçalves
Partner, IT Advisory
T: +351 210 110 012
E: ruigoncalves@kpmg.com

Cristina Alberto
Director, Business Continuity
T: +351 912 147 610
E: calberto@kpmg.com

A informação contida neste documento é de natureza geral e não se aplica a nenhuma entidade ou situação particular. Apesar de fazermos todos os possíveis para fornecer informação precisa e actual, não podemos garantir que tal informação seja precisa na data em que for recebida/conhecida ou que continuará a ser precisa no futuro. Ninguém deve actuar de acordo com essa informação sem aconselhamento profissional apropriado para cada situação específica.

© 2018 KPMG Advisory - Consultores de Gestão, S.A., a firma portuguesa membro da rede KPMG composta por firmas independentes afiliadas da KPMG Internacional Cooperative ("KPMG Internacional"), uma entidade suíça. Todos os direitos reservados. Impresso em Portugal. O nome KPMG e o logótipo são marcas registadas ou marcas registadas da KPMG Internacional.