BACKUP E DISASTER RECOVERY

DA TEORIA À PRÁTICA

TELECOM

ÍNDICE

INTRODUÇÃO

Garantir a operação da empresa com o mínimo impacto para os clientes e parceiros em situações de risco é uma preocupação para todos os gestores. Fazendo as contas, o custo associado aos riscos de falha de sistemas ou de perda de dados é mais alto do que o custo de manter plataformas de backup e de disaster recovery.

As contas são fáceis de fazer pelos gestores e a consciência de que é preciso agir sobre estas matérias ganha ainda mais importância se considerarmos o cenário de inovação tecnológica que a mobilidade ou o IoT (internet of things) estão a formar, e no qual a centralização segura da informação e a rastreabilidade dessa informação e de quem a ela acede é mais importante do que nunca.

No ambiente competitivo empresarial, que funciona 24/7, as organizações não se podem dar ao luxo de fechar durante um dia devido a desastres naturais ou ataques de cibercriminosos com o fim de roubar dados. Da mesma forma, lojas online ou operações virtuais não podem falhar ou colocar em standby transações. Um negócio sem dados não sobrevive, mas sem infraestrutura também não. Um downtime nos sistemas pode representar perdas avultadas para uma organização, a sua sustentabilidade ou até mesmo colocar em risco a sua reputação.

É fundamental que os gestores estejam preparados para responder a qualquer eventualidade de segurança ou de inoperacionalidade, devendo por isso planear possíveis cenários e planos de recuperação de desastres e incidentes que lhes permitam em pouco tempo recuperar dados ou sistemas e, desta forma, minimizarem os danos.

CONTINUIDADE É CRESCIMENTO

As empresas enfrentam diariamente todo o tipo de desafios económicos, mas a gestão da proteção da sua informação e dos seus sistemas está hoje nas agendas dos gestores, que para além do crescimento, procuram também assegurar a continuidade das operações.

Risco e resiliência são dois conceitos constantemente presentes no dia-a-dia de qualquer empresa. Das falhas de segurança aos ataques de ransomware, passando pelos desastres naturais e pelas falhas humanas, as preocupações da gestão são muitas e de naturezas distintas.

De acordo com o **estudo de Continuidade do Negócio da KPMG Portugal**, realizado entre setembro e novembro de 2017, através de dois questionários que inquiriram perto de 80 gestores portugueses responsáveis pela Continuidade do Negócio nas suas organizações, no topo da lista de preocupações dos gestores estão os incidentes de cibersegurança (90% dos inquiridos) e a falha das tecnologias de informação (78%), em comparação com outros eventos de risco como a falha dos fornecedores críticos da cadeia de valor, a falha de utilities, incêndios, terrorismo ou desastres naturais.

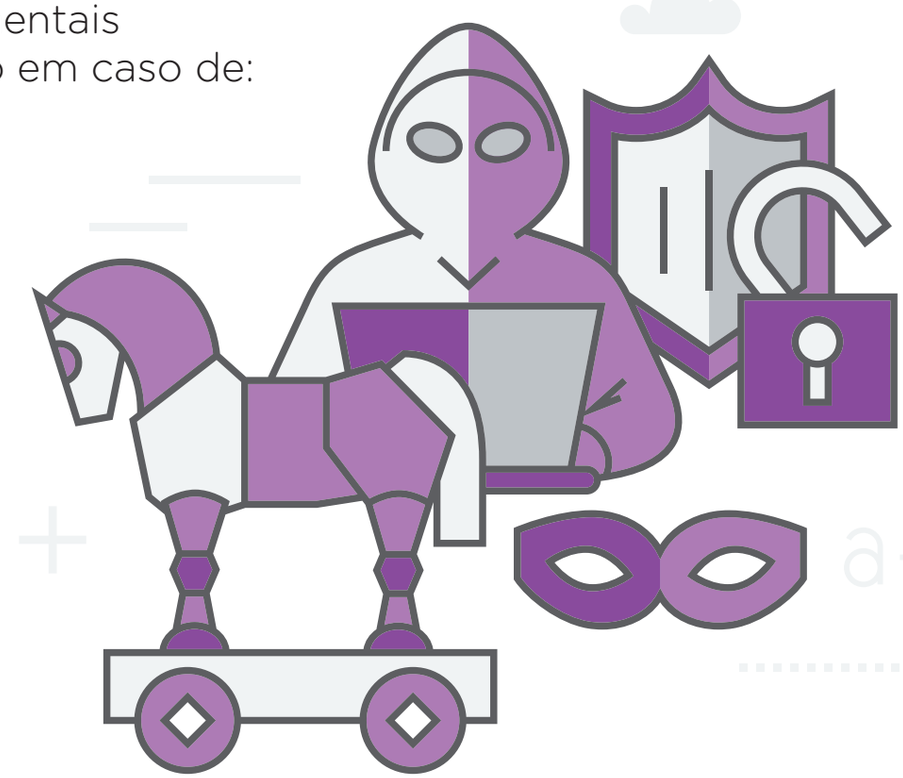
Para criar um plano eficaz de disaster recovery, os gestores devem adotar ferramentas e processos que lhe permitam responder rapidamente a situações de desastre e incidentes inesperados, como por exemplo:

- **Catástrofes naturais**
- **Cibercrimes, ataques de vírus/malware/ransomware**
- **Roubos de equipamentos ou de informações sigilosas**
- **Ataques terroristas**
- **Erros humanos**

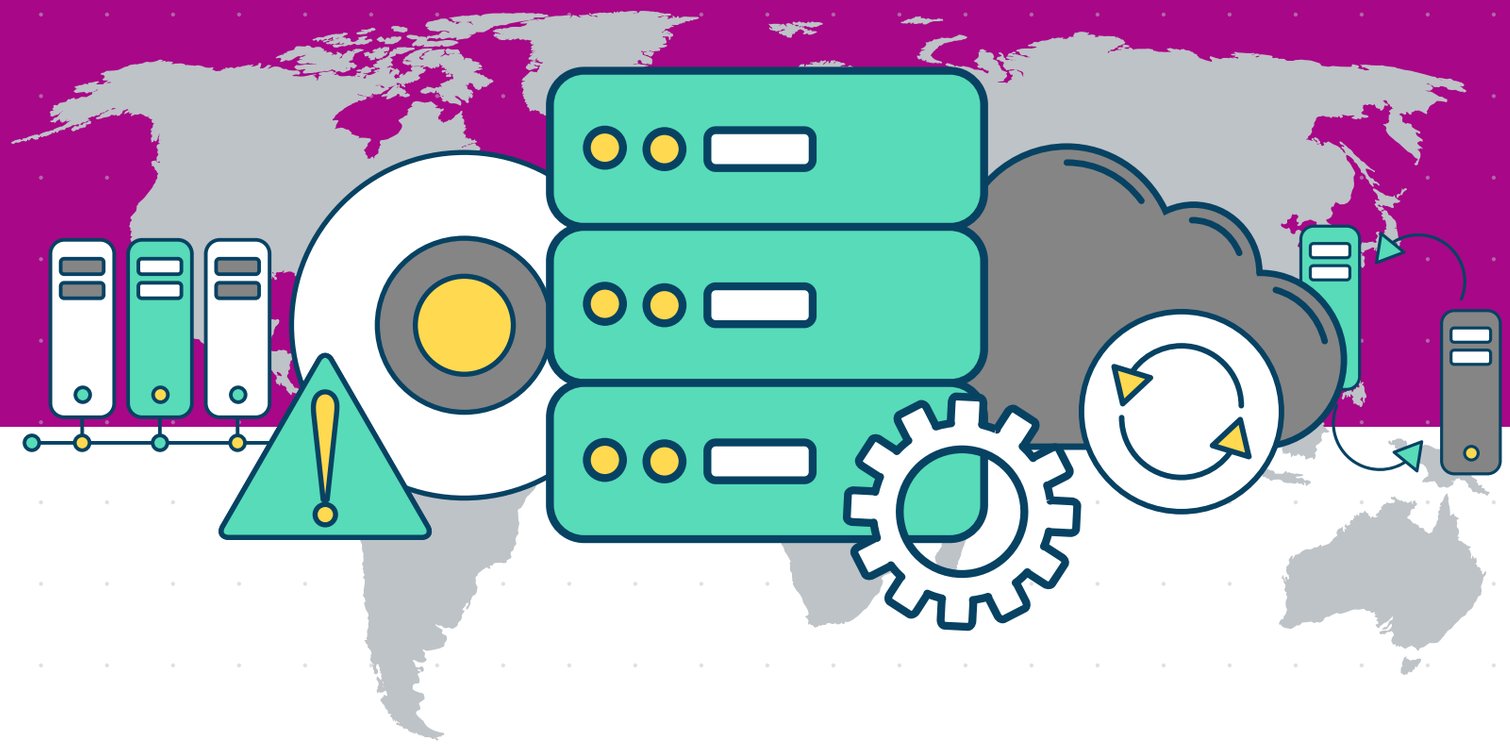
No estudo da KPMG Portugal, 90% dos inquiridos estão preocupados com incidentes de cibersegurança e 83% com a disrupção das TIC. Já 71% revela-se preocupado com as falhas ao nível das utilities, 71% com incidentes de saúde e segurança no trabalho, 66% com incêndios, 56% com terrorismo e 46% com desastres naturais.

Um plano de disaster recovery possui vários componentes fundamentais para garantir a continuidade do negócio e restabelecer a operação em caso de:

- **Perda de um sistema (sistema operativo ou falha de hardware)**
- **Perda de um ou mais servidores**
- **Perda de um ou mais data centers**
- **Perda de um site**
- **Perda de dados (eliminação ou degradação de dados)**
- **Inoperacionalidade de processos de negócio**
- **Serviços de TI indisponíveis**
- **Falhas de comunicações ou de energia**



BACKUP VS DISASTER RECOVERY



Não existem fórmulas fechadas que garantam um antídoto eficaz no caso de uma organização ser afetada por um ciberataque, uma catástrofe natural ou um ataque terrorista. Mas, há decisões de investimento que só podem ser tomadas se tiverem conhecimento dos recursos que existem disponíveis para que um gestor possa, de forma consciente, preparar melhor a sua empresa para as eventualidades do futuro.

O backup é visto como uma garantia da segurança das informações que uma empresa necessita, no entanto no caso de uma catástrofe ou incidente grave de segurança não é suficiente, pelo menos não sozinho, até porque perante uma catástrofe eminente a infraestrutura pode falhar e a informação que deveria ser salvaguardada fica perdida. Quanta informação está um gestor disposto a perder? De que serve uma solução de backup se não estiver integrada num plano de recuperação de desastre e continuidade?

O backup é o local a partir do qual a recuperação será feita. Este tipo de solução envolve muito mais do que simplesmente guardar a informação crítica, sendo neste ponto que a recuperação começa e o restauro das operações acontece, idealmente, no menor curto espaço de tempo possível.

QUAL SERÁ A MELHOR SOLUÇÃO DE BACKUP?

A dúvida está entre escolher um ambiente físico ou um ambiente virtual para armazenar o backup. Com o desenvolvimento da cloud, esta via tem-se afirmado como a melhor solução para as empresas guardarem os seus dados, mas há ainda alguns gestores que continuam a preferir os ambientes físicos e on-premises.

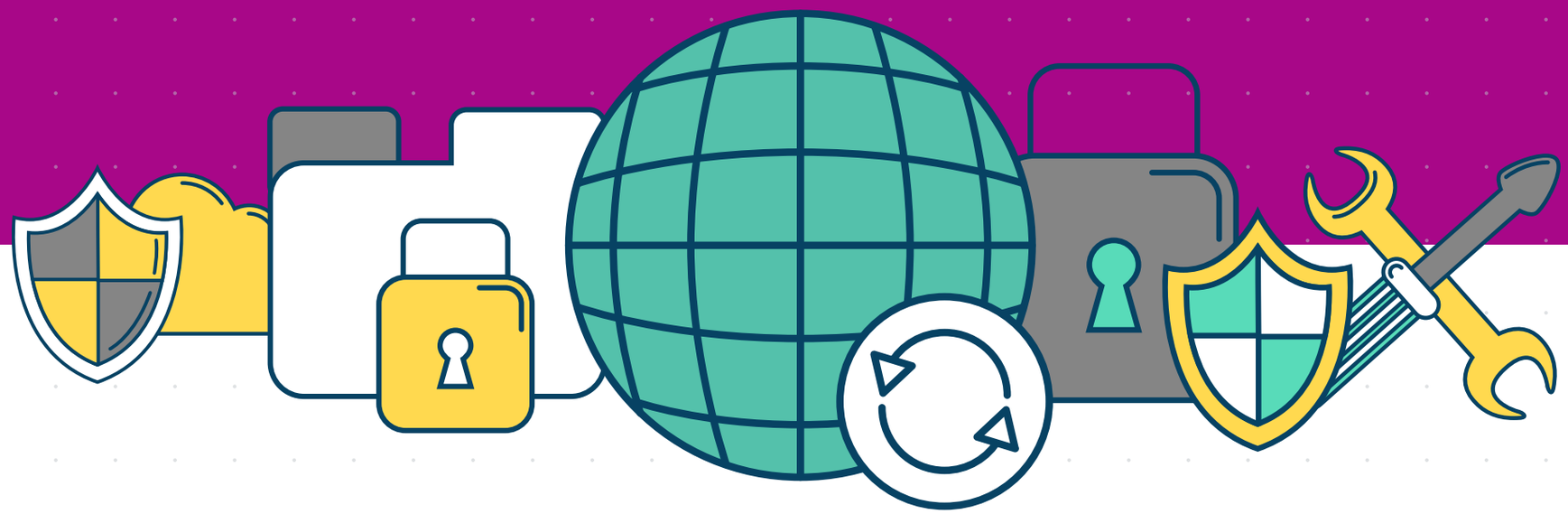
Por um lado, o backup on-premises continua a ser uma opção para gestores e IT Managers que preferem manter a sua informação num ambiente físico. Este modelo requer a aquisição de mais hardware, de modo a garantir espaço para os backups e uma arquitetura redundante. O facto de os backups ficarem alojados num diferente hardware garante uma maior redundância em caso de desastre.

Por outro lado, a flexibilidade, a segurança e o custo benefício associados aos ecossistemas virtuais continuam a atrair mais volume de dados para a cloud.

Antes de contratarem um serviço de backup na cloud, as empresas devem:

- **Identificar o espaço que vão necessitar**
- **Analisar os vários fornecedores, os serviços disponíveis e os planos de preços**
- **Validar se possuem um serviço de internet que permita ter boa performance na transferência dos dados**
- **Decidir a periodicidade da sincronização**
- **Definir as métricas RTO, RPO e RTA, que veremos mais à frente neste eBook**

O SEGURO ESCREVE-SE COM UM PLANO DE DISASTER RECOVERY



Para não serem apanhados desprevenidos, os gestores não podem esperar que aconteça um evento imprevisto para agir e proteger o seu negócio. Pensar num plano de recuperação só depois de algo acontecer pode ser tarde demais.

Nesta situação, como em muitas outras, estar atento e preparado para responder a uma inevitabilidade representa uma vantagem competitiva imensurável. Assumir que as probabilidades de não acontecer são mais fiáveis do que a proatividade de um plano bem definido e implementado é um risco que não devem ousar correr.

Para desenvolver um plano de disaster recovery é preciso isso mesmo, um plano. Planear bem a recuperação e restauro dos recursos computacionais que asseguram os processos vitais de processamento de dados, no menor tempo possível a fim de evitar impactos negativos no negócio.

Mas muito mais do que a mera recuperação e restauro da informação, falamos aqui de uma solução mais completa e eficaz. O plano deve contemplar a possibilidade de uma rápida recuperação da informação, mantendo constantemente atualizado um clone do site principal ou offsite.

Este plano de recuperação não deve ser uma iniciativa exclusiva de uma área ou de outra, mas de toda a organização, sendo o objetivo central proteger a continuidade do negócio da empresa.

1ª fase: **Preparação**

Uma avaliação profunda e completa de toda a infraestrutura de TI, dos ativos que compõem a organização, incluindo hardware, software, dados, comunicações, entre outros, é essencial antes de pensar um plano de recuperação. Só a partir de uma análise minuciosa e atenta é possível conhecer a situação real da organização e dos ativos imprescindíveis para o seu bom funcionamento, bem como das vulnerabilidades.

Num ambiente convencional para que o negócio possa continuar a desenvolver-se sem problemas não é só necessário recuperar dados, como também servidores, redes, workloads, máquinas virtuais, aplicações, etc.

ONDE ESTÃO OS DADOS E AS CHAVES PARA OS PROCESSOS?

Nos dias de hoje, o mais habitual é que, dentro de uma mesma organização, a informação esteja distribuída não só nas tradicionais instalações on-premise, nos postos de trabalho, nos dispositivos móveis, mas também algures na, ou, nas clouds.

Um plano de disaster recovery deve contemplar todos os pontos e no final responder a algumas questões, nomeadamente:

- **Qual é a capacidade real de recuperação da organização?**
- **Quanto tempo demoraria a recuperar?**

Se o IT Manager não conseguir responder a estas questões, então é preciso agir, porque a operacionalidade do negócio da sua empresa está em risco.

2ª fase: **Um plano com outros planos dentro**

Um plano de disaster recovery não vale nada se não contemplar todas as componentes organizacionais que têm de ser preparadas para que a recuperação seja, realmente, efetiva.

Mas, antes de tudo, as equipas de gestão e de TI devem identificar e formar uma equipa interna, que poderá ou não envolver um parceiro externo, que entrará em ação em situações de crise. Será essa equipa que fará uma primeira avaliação dos eventuais danos, após o incidente, procurando minimizar o impacto através da aplicação das medidas previstas no plano.

- **Plano de gestão de crise** – este plano deve ser desenvolvido pela equipa de TI e de gestão. Deve identificar todos os processos e dados, priorizando a sua recuperação em função da criticidade para a operação do negócio. A nomeação de uma equipa de gestão de crise é essencial.

- **Plano de continuidade operacional/negócio** – deve detalhar o que cada membro da equipa tem de fazer, em função das prioridades definidas, para colocar o negócio a funcionar enquanto se recupera do desastre. Será a equipa de gestão de crise que assumirá o comando a partir daqui.

- **Plano de recuperação de desastres** - vai colocar em prática o plano de continuidade operacional, após os incidentes, assegurando a operacionalidade do negócio e das atividades da organização, com o mínimo impacto nos processos ou transações. A partir daqui são implementadas medidas preventivas de perdas e danos, promovendo-se a recuperação rápida da situação de normalidade.

3ª fase: **Implementar passo a passo: prevenir em vez de remediar**

Cada tipo de negócio terá as suas prioridades e objetivos quer de segurança, quer operacionais. É com base nelas que se desenham estratégias de disaster recovery e se definem métricas. Mais do que apenas recuperação, a estratégia deve ser assumida como um conjunto de medidas preventivas de perdas e danos em caso de incidente. Numa estratégia de disaster recovery há varias questões que têm de ser respondidas através de ações concretas e bem definidas:

- **Quem são as pessoas chave? – alinhar perfis resilientes e procedimentos de recuperação.**

- **A segurança das pessoas está garantida? - quando se elaborar uma estratégia de disaster recovery deve-se minimizar o impacto dos incidentes para as pessoas quer a nível de segurança digital, quer física.**

- **Onde estão alojados os backups? – salvaguardar os dados/informação em mais do que uma localização é uma boa estratégia. A cloud é uma ótima solução para armazenar os backups.**

- **Qual é a infraestrutura mínima? – ter os recursos estritamente necessários para o funcionamento operacional do negócio bem identificados pode ser uma forma de não desperdiçar recursos valiosos na recuperação.**

- **Que métricas usar na recuperação?**
  - **RPO – define o ponto a partir do qual se quer fazer a recuperação, com as eventuais perdas de informação após o incidente bem identificadas.**
  - **RTO – é o período máximo de tempo de recuperação de aplicações de negócio ou dados. O RTO é definido a partir de uma análise de impacto de negócio (BIA – Business Impact Analysis).**
  - **RTA – ou Recovery Time Actual é o período de tempo que é necessário para ativar os planos de recuperação de negócio e continuidade numa situação de emergência.**

4ª fase: **Formação**

Além da descrição detalhada da responsabilidade de cada profissional envolvido no plano de disaster recovery, a empresa deve estabelecer mecanismos de formação, de modo a que todos os elementos operacionais possam estar sempre atualizados e sejam capazes de garantir a correta execução do plano em caso de necessidade.

Através de ações de formação periódicas é possível ter dentro de portas profissionais com as qualificações necessárias para conduzir a restauração. Pontos como o enquadramento legal, a identificação de riscos, de ameaças e vulnerabilidades, o planeamento da gestão de crise, a comunicação interna ou o plano de recuperação do negócio devem estar bem compreendidos pelos funcionários.

5ª fase: **Simulacros**

Se as ações estiverem automatizadas e forem convenientemente testadas todo o plano será implementado sem falhas. Atendendo ao facto de que os ambientes de negócios e de processamento de dados atuais são altamente dinâmicos, é essencial que o plano de recuperação de desastres seja cuidadosamente testado e avaliado semestralmente ou pelo menos uma vez por ano.

Desta forma, a empresa assegura que qualquer equipa de operações consegue executar o plano. O objetivo dos testes ou simulações é validar o plano de recuperação e fazer as correções necessárias. As empresas não devem esperar pelo dia "D" para verificar se tudo funciona a 100%. É preciso ir testando.

Destes testes, devem sair relatórios detalhados com dados sobre todos os tempos de execução dos processos e as falhas detetadas. Os utilizadores também deverão produzir relatórios com eventuais problemas que identifiquem na operação diária e sugerirem possíveis melhorias a adotar.

6ª fase: **Plano de continuidade**

Devido às mudanças diárias nos sistemas da organização com adição de novos sistemas, migrações de servidores, serviços ou outros, é necessário rever semestralmente o plano de continuidade com o intuito de garantir que o mesmo está de acordo com as necessidades da empresa e com o definido no plano de DR inicial. Manter um plano de continuidade atualizado exige sempre a análise de impacto no negócio e um acompanhamento constante de todas as alterações que sejam realizadas ao nível dos processos ou dos componentes técnicos da organização.

Um plano de continuidade deve obrigatoriamente responder a três questões:

- **Quais são os principais riscos/ameaças?**
- **Que impacto estes riscos/ameaças podem ter no negócio?**
- **Quais as decisões/ações que devem ser tomadas para que a operação do negócio seja garantida em caso de ataque?**

As organizações que possuem um plano de continuidade de negócio bem pensado e estruturado, garantem a sua capacidade de resposta em caso de eventos inesperados e, consequentemente, a sustentabilidade do seu negócio.

DRAAS – A RESILIÊNCIA QUE VEM DA CLOUD

Todas as estratégias de recuperação de incidentes são viáveis, desde que bem planeadas, testadas e implementadas. Mas soluções de disaster recovery as a service (DRaaS) chegaram para conquistar terreno a todas as outras. A Gartner prevê que o mercado DRaaS cresça numa proporção de 25% anual, nos próximos anos.

A ideia de imaterialidade da cloud que no início assustou os gestores e IT managers, deslumbrou-os mais tarde pela eficácia que pode proporcionar em muitas situações operacionais, mas também ao servir de base para as estratégias de disaster recovery, com toda a eficiência que mostrou ser capaz de proporcionar.

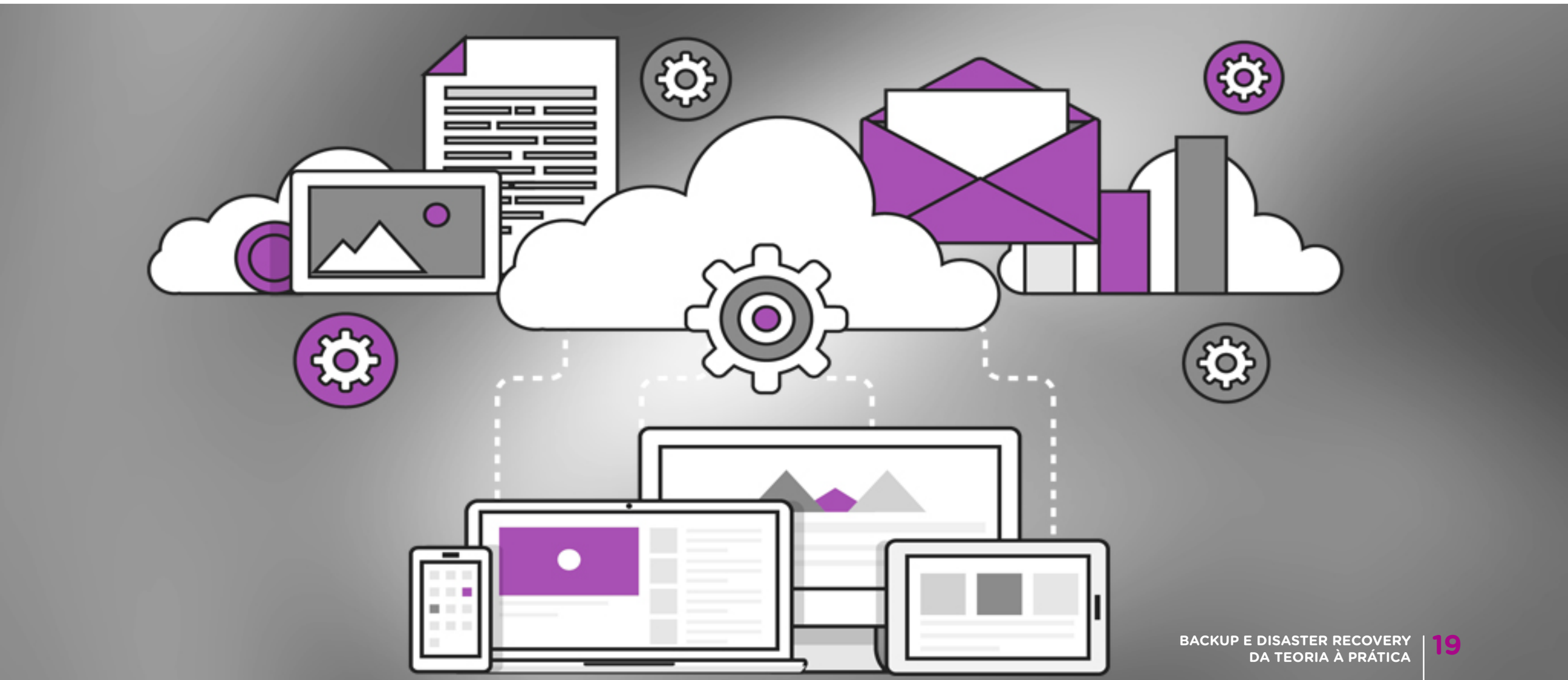
Pagar uma fatura de utilização de um serviço, dispensando os investimentos em hardware, licenciamento de software e outros custos fixos, fala mais alto na hora de fazer contas aos orçamentos. Mas as vantagens são muitas mais. A total flexibilidade, simplificação de processos e a segurança dos backups na cloud, permitem que após uma catástrofe a informação fique novamente disponível em tempo recorde.

O DRaaS permite também:

- **Melhor gestão de planos de disaster recovery – o facto de todos os planos estarem prontos a desencadear, a partir de um local remoto, facilita a sua execução e coordenação.**
- **Melhor utilização dos recursos de hardware – sem estar dependente de software ou hardware on-premises elimina as condicionantes à atuação da equipa de recuperação, que pode controlar todo o processo com base em máquinas virtuais.**
- **Melhor disponibilidade das aplicações – na cloud as aplicações continuam a funcionar, sem grandes impactos para a operacionalidade dos processos de negócio.**
- **Redundância – com os dados/informação guardada em múltiplas localizações, a segurança sai a ganhar e o negócio também.**
- **Backups automatizados – sem botões ou complicações. O upload de informação feito automaticamente e em tempo real, agilizando o tempo para a recuperação de aplicações de negócio ou dados.**

A estas vantagens é inerente o facto de não ser necessário reconstruir todo o sistema informático das organizações, desde os servidores à instalação de software e aplicações dedicadas. A virtualização potenciada pela cloud permite que todos os sistemas funcionem fora da empresa, o que reduz, significativamente os tempos de recuperação das operações de qualquer empresa que seja confrontada com um evento de segurança ou catástrofe ambiental.

O reforço tecnológico e operacional é assegurado por um plano de alocação de recursos dimensionado de acordo com as exigências de cada evento, sendo executado em tempo real.



CHECK-LIST: DA TEORIA À PRÁTICA

Embora a construção de um plano de disaster recovery dependa das especificidades de cada negócio, existem pontos que são relativamente comuns e que devem ser contemplados pelo IT Manager na definição de uma estratégia de recuperação de dados e mitigação de risco.

Para simplificar o processo de criação do plano de disaster recovery criámos uma check-list com os principais passos.

Tarefa	Descrição
Criar fluxograma de sistemas informáticos empresariais	Fluxograma com a descrição de todos os serviços críticos da organização. Desta forma é possível perceber que elementos devem ser considerados no dimensionamento do site de DR.
Dimensionar o site de DR na cloud	Dimensionamento dos recursos necessários. Servidores, RAM, CPU, storage, networking, largura de banda.
Nomear um responsável de operação do plano de DR	Definição do responsável pela gestão de todas as equipas no plano de DR.
Nomear um responsável de operação dos utilizadores	Definição do responsável por instruir e apoiar os utilizadores com o plano de DR em execução.
Implementar o plano de DR	Implementação do Plano de DR com base no assessment realizado e recursos adquiridos.
Efetuar testes de implementação do plano de DR	Realização de testes de modo a garantir que o plano está bem dimensionado e que todas as instruções de execução estão bem descritas e sem falhas. Devem ainda ser registados todos os tempos, problemas e métricas de performance.
Elaborar relatório de implementação	Relatório final com referência a todos os problemas detetados durante o teste de DR.
Formação das equipas de operação	Formação às equipas de operação de como executar os planos de DR, mitigar os problemas atuais, prevenir as perdas de dados durante a ativação do DR, bem como a reposição dos dados após roll-back do Offsite.
Formação dos colaboradores	Formação aos colaboradores de como proceder para aceder às aplicações em DR (ligação de VPN, novos links de acesso a aplicações, etc.) e de como reportar não conformidades.
Simulacros	Realização de simulacros para testar a integridade do plano de DR em produção e colmatar possíveis falhas existentes ou melhoria do plano em produção.
Plano de continuidade	Idealmente deve ser feito um assessment a cada 2 meses de forma a ter o plano de DR atualizado bem como o fluxograma dos sistemas informáticos. No fim do assessment devem ser implementadas as alterações necessárias.

CONCLUSÃO

Seja um desastre natural que bate à porta de um data center ou um ciberataque que desligue os sistemas críticos de uma empresa, os prejuízos que podem ser contabilizados são incalculáveis. Basta olhar para o passado recente e relembrar os efeitos do WannaCry em Portugal, que obrigou a desligar sistemas informáticos de grandes entidades públicas e privadas nacionais, ou há uns anos atrás, para os ataques às empresas SONY, Ashley Madison, Yahoo, entre outras.

Sem políticas e procedimentos que garantissem a recuperação e operação das infraestruturas de TI e a disponibilidade da informação, nenhuma empresa conseguiria em tempo útil, e com reduzido impacto, sobreviver a estes incidentes imprevistos.

Com as portas abertas para a web, as empresas devem considerar a implementação de planos de disaster recovery e de continuidade com a plena consciência que o investimento já não os deverá separar desta estratégia. A cloud veio permitir democratizar a implementação deste tipo de projetos e hoje é possível dimensionar os planos à medida da realidade de cada empresa, sejam pequenas, médias ou grandes.

A continuidade do negócio deve sobrepor-se nas agendas dos gestores, que deverão aprender como as estratégias de disaster recovery podem ser aplicadas nas suas organizações, quer através da análise de resultados de casos de sucesso, quer através de consultas a especialistas que se posicionam neste mercado.

É importante que na definição de uma estratégia de disaster recovery, as empresas possam contar com um parceiro que ajude a pôr em marcha o plano e que possa aconselhar a implementação da resposta durante uma crise/ataque. A escolha do fornecedor certo é determinante para o sucesso de toda a operação.

Ar Telecom reúne 18 anos de experiência no mercado e pode ser o Parceiro ideal do IT Manager na definição do plano de disaster recovery. A Ar Telecom é especialista em:

SOLUÇÕES DE DISASTER RECOVERY AS A SERVICE.

SOBRE A AR TELECOM

Ambicionamos ter a oferta mais completa de serviços de cloud do mercado nacional, proporcionando condições às empresas para ousarem desafiar novos mercados e soluções.

Disponibilizamos uma oferta completa de serviços cloud, para que o departamento de TI de cada empresa se dedique a projetos estratégicos e que exigem recursos focados e dedicados.

Computação (cloud privada e cloud pública), Backup e Disaster Recovery, são as principais áreas de serviços cloud em que a Ar Telecom pode apoiar o negócio das empresas.

O conhecimento das especificidades de cada setor de atividade, para melhor adequar as soluções às necessidades de cada cliente, é uma das garantias dadas pela Ar Telecom.

Precisa de ajuda?

ENTRE EM CONTACTO CONNOSCO!