GUIA COMPLETO SOBRE A CONTINUIDADE DE NEGÓCIOS

CentralServer

INTRODUÇÃO

É como já diz o velho ditado: **"a vida é uma caixinha de surpresas"**. Toda companhia, independentemente do seu tamanho ou do ramo de negócios, está sujeita a eventuais adversidades ou interrupções que podem comprometer — e muito! — o bom andamento das suas operações.

Já imaginou o que poderia ocorrer se a sua empresa ficasse sem internet ou energia elétrica por várias horas? Ou, pior, se algum imprevisto inviabilizasse a operação por dias e dias a fio?

Pode até parecer que a possibilidade dessas coisas acontecerem é pequena, mas a verdade é que estamos todos vulneráveis aos mais diversos incidentes. Desastres naturais, incêndios, falhas nos sistemas e vários outros episódios podem acontecer a qualquer momento e quando menos esperamos — e é justamente aí que surge a pergunta: **como você pode garantir a continuidade da sua empresa nesses casos extremos?**

NEM TUDO ESTÁ PERDIDO

A boa notícia é que esse cenário pode ser evitado. Foi pensando em todas essas questões que resolvemos produzir este eBook, um **guia completo no qual você encontrará uma série de informações relevantes sobre o conceito de Gestão de Continuidade de Negócios.**

Você verá aqui a importância de se preparar para essas adversidades, **aprenderá como elaborar um planejamento estratégico e entenderá a estrutura de um plano de continuidade**. Além disso, mostraremos também um passo a passo de como realizar um plano de contingência, apresentando a você conceitos como o BC/DR — que engloba, além da continuidade do negócio, a capacidade de recuperação de desastres.

Ufa! Depois dessa introdução digna de um filme-catástrofe de Hollywood, sugerimos que você acompanhe as nossas dicas com muita atenção e, ao final, **comece a implantar esses conceitos também na sua empresa.**

Boa leitura!

O PLANEJAMENTO DA CONTINUIDADE DE NEGÓCIOS

Qualquer evento ou incidente extremo **requer uma resposta imediata de toda a empresa**. Contudo, isso precisa acontecer de maneira estruturada, rápida e precisa, até para que os impactos negativos sejam evitados ou reduzidos.

É justamente para permitir essas ações coordenadas que existe o **Plano de Continuidade de Negócios** (ou **PCN**, como é mais conhecido). Ele é um conjunto de estratégias e medidas preventivas que garante o funcionamento das atividades vitais de uma empresa durante uma situação extrema, até que tudo seja normalizado.

DEFININDO O SEU PCN

Além da prevenção, é preciso também definir todos os processos que devem acontecer em uma situação-limite, a fim de recuperar os negócios e continuá-los o mais rapidamente possível.

Por mais que o núcleo de um Plano de Continuidade de Negócios seja composto das mesmas diretrizes, é natural que sofra algumas **alterações de empresa para empresa**, variando de acordo com a essência do negócio. Por isso, os gestores responsáveis precisam focar em **três questões fundamentais** ao elaborar o PCN de suas corporações.
São elas:

Análise de risco: quais são as principais ameaças que podem levar à ruptura das atividades da empresa?

Análise de impacto: de que maneira essas eventuais ameaças podem impactar o seu negócio?

Planejamento estratégico: caso a ameaça se concretize de fato, o que deverá ser feito para que a empresa retome as suas operações?

ESTRUTURANDO UM PLANO DE CONTINUIDADE DE NEGÓCIOS

Após as análises e o planejamento, já é possível começar a estruturação do PCN. Ele é normalmente composto de quatro **subplanos** ligados entre si, sendo que cada um representa um estágio diferente. Conheça-os:

PLANO DE CONTINGÊNCIA

Este plano deve ser utilizado apenas em último caso, quando todas as medidas de prevenção tiverem falhado. Ele **define as necessidades e ações mais urgentes**.

PLANO DE ADMINISTRAÇÃO DE CRISES (PAC)

Aqui, são definidas as **funções e responsabilidades dos times envolvidos** na implantação das ações de contingência — antes, durante e após o incidente.

PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

Neste plano é feito o planejamento para que, uma vez controlado o incidente e **passada a crise**, a empresa possa retornar o mais rápido possível aos seus níveis originais de operação.

PLANO DE CONTINUIDADE OPERACIONAL (PCO)

Já aqui, seu objetivo é **restabelecer a normalidade** de todos os ativos necessários para o bom andamento das operações da empresa, reduzindo o tempo de indisponibilidade e os impactos provocados por um eventual incidente — a queda da conexão da internet é um bom exemplo.

É muito importante que um **time multidisciplinar** esteja envolvido na elaboração dos planos — afinal, eles serão aplicados em toda a organização. Além disso, por questões de segurança, recomenda-se o treino de, pelo menos, duas pessoas em cada plano de continuidade.

Ao validá-los e aprimorá-los continuamente, a empresa assegura a elevação do seu nível de maturidade e consolida a confiança de todas as partes envolvidas.

A RECUPERAÇÃO DE DESASTRES NAS EMPRESAS

Como vimos anteriormente, o Plano de Recuperação de Desastres visa retomar, o mais rápido possível, todos os processos vitais para o funcionamento do negócio — ainda que com desempenho reduzido.

Um **PRD eficiente** precisa conter todas as ações necessárias para que isso aconteça, de forma que não haja muitos prejuízos e os resultados da empresa não sejam permanentemente prejudicados.

Podemos dizer que, apesar de pretender a retomada de todos os processos operacionais, **o foco do PRD está principalmente na segurança das informações da empresa**. Afinal, uma falha no principal data center ou a mera extinção dos servidores remotos podem causar transtornos irreparáveis — e, às vezes, podem significar a ruína da corporação.

Para que isso seja evitado, apresentamos a seguir três ótimas dicas que facilitarão muito a sua vida. Confira!

ATENTE-SE AO SISTEMA DE COMUNICAÇÃO DE DADOS

Hoje, todo o sistema de comunicação de dados de uma empresa trafega por uma conexão de internet. Essa conexão pode ser via banda larga ou internet dedicada, e cada empresa deve escolher o modelo ideal de acordo com as suas necessidades.

O **modelo via link dedicado** envia todos os dados em um canal único, o que torna a conexão muito mais rápida e estável. Na **banda larga**, porém, o tráfego das informações e a velocidade são compartilhados com todos os computadores e dispositivos conectados à rede, o que pode causar lentidão e instabilidade.

Para que o seu Plano de Recuperação de Desastres seja efetivo, um sistema de comunicação de dados ágil, seguro e eficiente é fundamental. **Uma boa alternativa, caso esteja disponível na sua região, é a veloz conexão em fibra ótica**.

IMPLANTE A REPLICAÇÃO DE DADOS E RECURSOS

Uma das melhores maneiras de garantir a segurança dos dados importantes e o sucesso do seu PRD é **trabalhar com a replicação (ou redundância) de arquivos e recursos.**

Ter um **data center primário** é uma boa medida preventiva, já que as suas fontes de energia são alternativas e evitam que os dados sejam perdidos ou corrompidos por causa de um blecaute, por exemplo.

Mas, se a empresa dispuser de recursos, é altamente recomendável **adotar também um data center secundário**. Dessa maneira, todos os dados e arquivos da corporação serão replicados, o que aumentará muito a segurança e tornará o Plano de Recuperação de Desastres ainda mais efetivo.

FAÇA BACKUPS REGULARES

A cópia de segurança dos arquivos, softwares e aplicativos deve ser feita regularmente. Só uma rotina de backup é capaz de impedir que dados importantes da empresa se percam devido a incidentes inesperados.

Também é fundamental **realizar testes periódicos que assegurem a qualidade da gravação**: já pensou descobrir, na pior hora possível, que todo o seu backup está corrompido?

Por precaução e para facilitar a disponibilidade, **as cópias físicas devem ficar em lugares diferentes**. Ainda assim, recomendamos fortemente que as cópias de segurança também sejam armazenadas na nuvem, em servidores digitais: além de muito prática, hoje essa opção é uma das mais acessíveis — o que é um alento e tanto para as pequenas e grandes empresas.

Como vimos, as medidas preventivas são essenciais em um Plano de Recuperação de Desastres. Porém, é importante que todos esses procedimentos sejam documentados: só a correta obediência a eles garantirá que as informações importantes para a empresa não se percam.

O BC/DR E OS PLANOS DE CONTINGÊNCIA

Tudo o que vimos até aqui faz parte de um conceito chamado **BC/DR — ou Business Continuity Disaster Recovery**, como é conhecida a Continuidade do Negócio e a Recuperação de Desastres na sua sigla em inglês.

No capítulo anterior, vimos em detalhes como atuar na Recuperação de Desastres — um trabalho realizado apenas após o acontecimento de um incidente extremo. Agora, veremos o que fazer antes disso, **quando o desastre estiver prestes a ocorrer** e todas as eventuais medidas de prevenção não tiverem surtido efeito.

DESENVOLVENDO O SEU PLANO DE CONTINGÊNCIA

Já vimos que é o **Plano de Contingência que define as necessidades e ações mais urgentes** da empresa ao enfrentar uma ocorrência grave. Ele tem como objetivo trabalhar as consequências do incidente e evitar que coisas piores aconteçam devido aos problemas gerados.

Mas o que deve fazer parte desse plano emergencial? Qual a melhor maneira de a empresa colocá-lo em prática? **Observe o nosso passo a passo a seguir e descubra!**

AVALIE E IDENTIFIQUE OS RISCOS

Você precisa estipular a **probabilidade de cada um dos riscos** acontecerem, bem como o impacto negativo que isso acarretaria.

AGRUPE OS RECURSOS

Faça um **levantamento de todos os recursos** humanos, técnicos, financeiros e logísticos que estejam a dispor para desenvolver o planejamento.

ORGANIZE AS ESTRATÉGIAS

Defina a ordem de ação para enfrentar cada uma das ameaças e **estabeleça uma metodologia** de trabalho para cada uma das situações que possam vir a ocorrer.

Determine ainda o que deverá ser feito caso os riscos detectados de fato aconteçam, começando pelas ameaças que mais tenham chances de se concretizar.

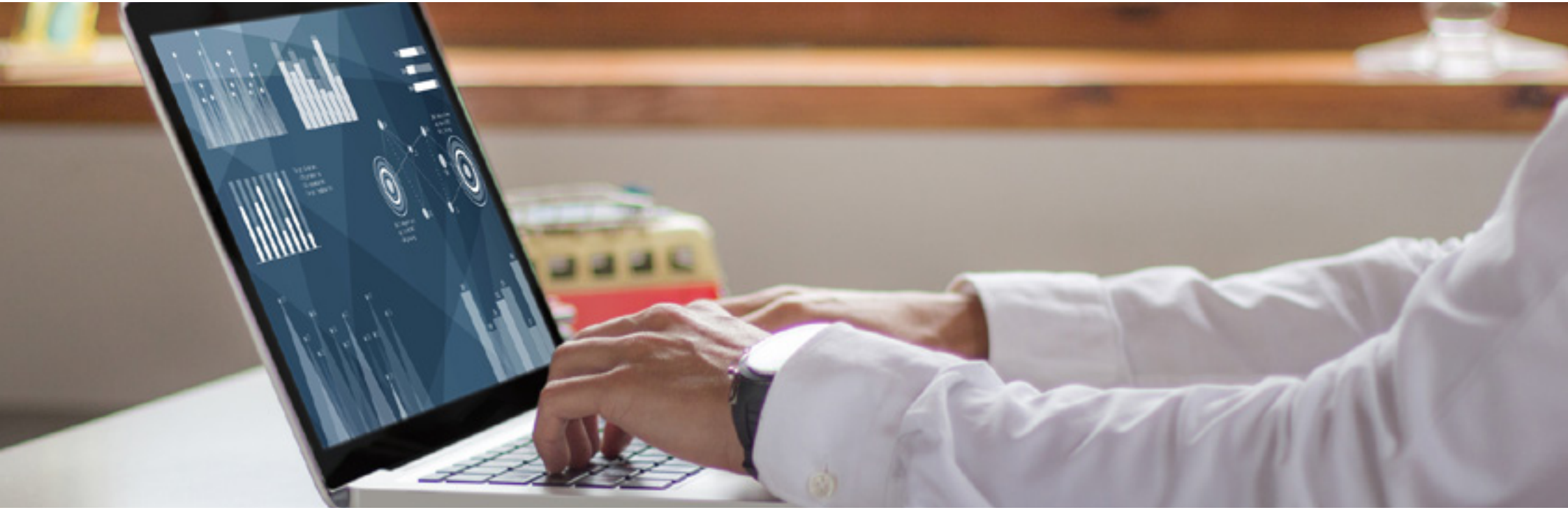
FAÇA UM BOM TREINAMENTO

É preciso **treinar com eficiência todos os indivíduos envolvidos no planejamento**. Aborde todos os desdobramentos possíveis de cada ameaça e demonstre claramente o que a empresa espera que seja feito. Realizar simulações periódicas de cada situação também é uma boa ideia.

AVALIE OS DESEMPENHOS

Cada vez que houver uma simulação ou real execução do plano de contingência, verifique se as metas foram plenamente alcançadas. Em caso negativo, saiba detectar os erros para que estes possam ser avaliados e corrigidos.

PREVINA-SE CONTRA AS FALHAS SISTÊMICAS



Hoje em dia toda empresa depende da TI e tem muito a perder quando ocorrem falhas generalizadas. E, quando isso ocorrer, saiba que somente a tecnologia não será capaz de resolver todos os problemas.

Por mais que você tenha um bom planejamento de BC/DR e o combine às melhores ferramentas da computação em nuvem, **uma proteção permanente contra falhas sistêmicas requer alguns procedimentos vitais**. Listamos três deles:

PLANO DE AÇÃO

Um plano de ação deve ter uma lista com os recursos essenciais para a continuidade do negócio em caso de falhas. **Você precisará definir o RTO** (Recovery Time Objective, ou o tempo máximo tolerável para que o sistema volte ao normal após uma falha) e o **RPO** (Recovery Point Objective, o tempo máximo de perda das atualizações de dados durante o processo de recuperação).

REDUNDÂNCIA DE RECURSOS

Como vimos antes, a replicação de arquivos e dados entre servidores de diferentes data centers é altamente recomendada. Essa solução deve admitir a **criação de vários pontos de restauração** e a definição do RPO e RTO.

TESTES PERIÓDICOS

Testes regulares são necessários para **simular as falhas** sem afetar a rotina de produção. É assim que você avaliará a eficácia do Plano de Ação e do sistema de redundância de dados, evitando surpresas desagradáveis caso algum desastre ocorra de fato.

O planejamento de BC/DR é um item essencial na estratégia de qualquer companhia dependente de TI. Com ele, a luta contra as falhas sistêmicas incentiva práticas de gestão que asseguram a continuidade do seu negócio.

CONCLUSÃO

E, com isso, chegamos ao final deste guia. Viu só como é importante ter a empresa preparada para lidar com imprevistos?

Aqui, **você viu como é importante estar preparado para lidar com eventos extremos**, bem como aprendeu a estruturar o seu próprio Plano de Continuidade de Negócios. Viu também um passo a passo para realizar o seu próprio plano de contingência e aprendeu o significado do conceito BC/DR, adquirindo a capacidade de não apenas continuar o seu negócio, mas também de se recuperar de eventuais desastres.

Se você ainda ficou com alguma dúvida sobre o assunto, não hesite em entrar em contato conosco, teremos o maior prazer em ajudar!
Um grande abraço e desejamos sucesso ao seu negócio!

A **CentralServer** fornece serviços de computação em nuvem corporativa com base em tecnologias de referência, melhores práticas e infraestruturas de data center de alta disponibilidade.

Atuamos no modelo multicloud para oferecer o melhor mix de soluções em nuvem VMware, Azure e AWS.

Nossas soluções sob medida removem a complexidade da TI e vêm acompanhadas de um atendimento extraordinário para apoiar o crescimento do seu negócio.

Entre em **contato** conosco!