Capítulo 6

Plano de continuidade dos negócios

Neste capítulo conheceremos o conceito e a prática do plano de continuidade dos negócios. Atuando de forma estratégica, esse plano conta com processos bem definidos e uma análise profunda sobre as consequências para a empresa de ameaças que já existem ou possam surgir. Para nosso aprendizado, vamos conhecer a Análise de Impacto de Negócios (BIA) e também os Objetivos e Chaves de Resultados (OKRs).

1 Conceito de solução de continuidade dos negócios

A gestão de continuidade dos negócios se apresenta para identificar e gerenciar ameaças atuais e futuras aos negócios da empresa, adotando uma postura proativa para minimizar o impacto de incidentes.

Assim, será possível manter funções críticas em funcionamento, mesmo em períodos de crise, minimizando o tempo de inatividade durante incidentes e melhorando o tempo de recuperação.

Dessa forma, a empresa consegue apresentar resiliência aos seus clientes, fornecedores e em solicitações de propostas; afinal, uma instituição que a contratará saberá que o fornecedor tem uma empresa mais segura, que sabe lidar com momentos de crise e gerenciar problemas.

A certificação ISO 22301 – Sistema de gestão de continuidade de negócios é uma norma internacional baseada em requisitos que proporcionam segurança e resiliência para um negócio, independente de estrutura ou segmento. A certificação visa oferecer aos negócios ferramentas para controle e resguardo de situações extraordinárias (ABNT, 2020).

A ISO 22301 especifica os requisitos para que um sistema de gestão não apenas proteja os seus negócios contra incidentes inoportunos, mas também reduza as possibilidades destes ocorrerem e garanta que a sua empresa se recupere, caso aconteçam (ABNT, 2020).

A ABNT (2020) define a ISO como um componente que especifica pontos que podem ser implementados pela empresa, a fim de protegê-la, reduzir ameaças e saber responder e se recuperar de momentos críticos.

Os benefícios da continuidade dos negócios envolvem questões como: processos e sistemas bem desenvolvidos, capazes de identificar pontos críticos e impactos que podem ocorrer no caso de problemas; bons níveis de capacitação na resolução de problemas; uma boa

imagem perante clientes e concorrentes; afinal, são capazes de se recuperar de crises de forma eficiente; impacto financeiro controlado; credibilidade e compromisso tanto com colaboradores quanto clientes.

As ameaças que podem acometer as empresas envolvem: falhas de sistema, sabotagens, pandemias, catástrofes, fraudes, roubos, assaltos, incêndios, entre outros acometimentos que afetam diretamente a operação da instituição.

Portanto, investir em estratégias de continuidade dos negócios é saber que sua empresa conseguirá continuar operando mesmo em momentos de crise e que os problemas serão resolvidos de forma rápida e efetiva, apresentando os três principais pilares da segurança da informação: confidencialidade, integridade e disponibilidade (BAARS et al., 2018).

2 Processo de desenvolvimento de planos de continuidade dos negócios

Para se organizar os planos de continuidade dos negócios, é importante conhecermos o ciclo de vida deste processo, composto pelas etapas:

- Avaliação de riscos: objetiva analisar as ameaças que podem acometer a segurança da empresa para se preparar para possíveis danos caso algum incidente ocorra.
- Análise de impacto nos negócios (BIA – business impact analysis): visa quantificar os impactos decorrentes dos possíveis incidentes, com base em entrevistas com gestores. Ela possibilita que a empresa saiba identificar ameaças que possam interferir na continuidade dos negócios, o tempo que a empresa consegue ficar sem operar de forma que seus negócios não sejam prejudicados e a infraestrutura básica que a instituição deve ter para planos de contingência.

- Estratégias de continuidade de negócios: objetiva desenvolver, implantar ou atualizar uma infraestrutura baseada na orientação dada pela alta direção. Neste momento, os responsáveis criam formas de analisar o ocorrido considerando os processos críticos e descrição das principais atividades, perfil dos colaboradores envolvidos, tecnologias que suportam as atividades que serão realizadas, impactos (financeiros, legais e operacionais), priorização dentro da gravidade do dano, consequências e tempo para recuperação.

- Desenvolvimento e atualização dos planos: deve incluir planos para resposta a incidentes ou emergências, de declaração da contingência, de gerenciamento de crise, de mobilização de pessoas, de comunicação interna e externa etc. Aqui, os responsáveis definem o projeto que será implantado, elaboram questionários para coleta de informações, entrevistam colaboradores envolvidos, determinam um tempo para recuperação e estabelecem um ponto real de recuperação (RPO – recovery point objective), ou seja, o que realmente poderá ser tolerado sem que haja um prejuízo maior à instituição.

- Exercícios e testes: a execução destes é fundamental para colocar em prática a estratégia traçada anteriormente.

Após as etapas acima citadas, é realizado o chamado ciclo PDCA. O ciclo é indicado para planejar, fazer, checar e agir para controlar todos os processos envolvidos na continuidade de maneira frequente. Ele se mostra uma maneira ampla e eficiente para auxiliar na execução de um plano estratégico, o qual deve ser elaborado previamente por uma equipe especializada. Ele auxilia, também, na melhora de resultados e desempenho da empresa, pois ajuda no monitoramento das execuções.

Portanto, o ciclo assessora na identificação de dificuldades, localização de problemas, definição do real problema, sugere possíveis soluções e analisa os pontos positivos e negativos dos planos aplicados.

3 Preparação do BIA e avaliação de riscos e impactos da continuidade dos negócios

Sabe-se que

> [a]s instituições, independente de tamanho ou setor de atuação, são sensíveis a interrupções nos seus processos de negócio. Elas são vulneráveis a situações de riscos, que são originadas por desastres naturais ou por pequenos incidentes, e a seus respectivos impactos. A ocorrência desses eventos pode causar uma interrupção parcial ou total das atividades da instituição, prejudicando seu negócio (FRIEDENHAIN, 2008, p. 11).

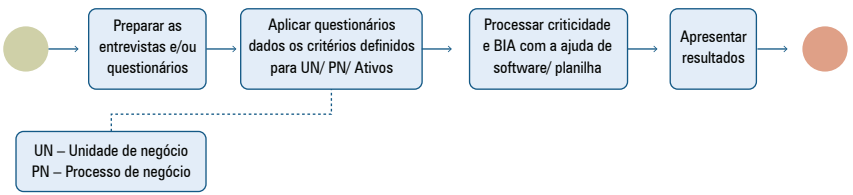
A preparação do BIA (business impact analysis) ajudará a identificar e analisar os processos da organização e os efeitos que uma interrupção do negócio pode acarretar. A empresa, assim, será capaz de saber quais são os processos mais críticos e em quais deverá atuar primeiro, além de conseguir determinar o tempo estimado para sua recuperação frente àquele problema.

Primeiramente, é definido o projeto, o qual determinará implantação, objetivos, escopo e prazo. A preparação de entrevistas e questionários subsidia a análise do BIA, auxiliando na identificação dos impactos e as paradas que aconteceram ao longo do tempo, recursos e ações necessárias para situações de crise. Elas envolvem funcionários envolvidos, custo, prejuízo em relação ao tempo de parada, aspectos legais e de imagem.

As entrevistas possibilitam esclarecimentos sobre questões que acontecem ou poderão acontecer que causam problemas para a empresa. Após processar as informações e definir suas criticidades (por meio

de um software), apresentam-se os resultados e se aponta o tempo de recuperação e o que pode ser feito para que nada se agrave e seja corrigido da melhor forma. Essas etapas estão representadas na figura 1.

Figura 1 – Análise de impacto de negócios – BIA



Fonte: adaptado de Instituto Federal de Santa Catarina (2018).

As entrevistas são necessárias para detalhamento do processo de negócio, ou seja, analisar os processos considerados críticos para direcionar a análise de impacto. Através dela é possível também identificar as perdas financeiras que podem ocorrer em casos mais graves, como paralisação de um processo e também o quanto a empresa despenderá para recuperar seu processo de negócio. A pessoa que prepara e realiza as entrevistas é o responsável pelas atividades críticas da empresa.

A aplicação de questionários, como o próprio nome já diz, é a real aplicação de questões relacionadas aos processos. Neles constam informações sobre os processos críticos, grau de criticidade dos sistemas, tempo máximo para paralisação, tempo estimado para paralisação e retorno das atividades e impactos a serem considerados. Ele apresenta uma escala qualitativa de impactos. Os questionários variam de acordo com a empresa e a área envolvida.

No caso de processamento da criticidade e a BIA, seria tabular os resultados referentes aos questionários e analisar a criticidade da situação e avaliar todas as consequências – financeiras, legais, operacionais, RH e imagem da empresa (PRIMÃO, 2018).

Por fim, temos a apresentação dos resultados que consiste no momento de estruturar, tabular tudo o que foi coletado e definir qual a real situação da instituição e quais serão as medidas tomadas diante dos resultados, a fim de dar uma resposta rápida à situação.

Primão (2008) reforça que, durante todo esse processo, a comunicação é a parte mais importante para o plano de continuidade dos negócios, pois somente apresentar dados pode não retratar as questões realmente relevantes.

4 Recursos críticos de TI

Os recursos críticos são os ativos que são fundamentais para a empresa operar em sua estrutura de TI de forma segura e eficaz. De acordo com Iwasa e Tavares (2017), podemos citar como exemplos de recursos críticos:

- confiabilidade (prestação de serviço com confiança e exatidão);
- responsabilidade;
- responsividade;
- segurança;
- empatia;
- tangibilidade.

Eles são o foco para realizar o trabalho de forma segura e garantir que a empresa esteja protegida.

Os recursos críticos – chamados desta forma, pois são essenciais para a sobrevivência da empresa – fazem parte dela e a auxiliam na boa execução dos ativos críticos, que nada mais é do que aquilo que tem valor tangível ou intangível para ela. Eles englobam desde máquinas e

instalações até hardwares e softwares. Isso significa que todos os setores da organização têm que estar em comunicação para que ameaças sejam evitadas e a operação não seja prejudicada (ALMEIDA, 2018).

As ameaças que podem atingir os ativos críticos podem ser de natureza humana ou ambiental. Recursos que influenciam na estratégia da organização são meios de alcançar melhores resultados para os seus negócios.

Portanto, de acordo com Almeida (2018), é importante que a proteção desses ativos e seu gerenciamento de forma adequada seja algo rotineiro na instituição. Descuidar de ativos, principalmente de tecnologia da informação, pode causar inúmeros problemas, como financeiros, e outros danos no negócio.

5 Manutenção dos planos de continuidade

De acordo com Dupont (2018, p. 3):

> Um Plano de Continuidade de Serviços de TI propõe mecanismos para auxiliar o conselho a garantir o funcionamento dos seus sistemas, com o foco em mitigar os impactos de desastre no menor tempo possível. Casos de catástrofes e acidentes causados por agentes externos (incêndios, enchentes, atentados e fenômenos da natureza) são possíveis causadores de indisponibilidade, e devem ser previstos e planejados para assegurar a contínua disponibilidade dos sistemas, além de uma série de vulnerabilidades às quais estão sujeitos os sistemas informatizados, como falhas de discos, quedas de luz etc.

Validar e atualizar a documentação criada no processo dos planos de continuidade é também uma importante tarefa do profissional que estará envolvido no gerenciamento de continuidade do negócio. Essa ação identificará melhorias no processo.

Ainda para a autora, as estratégias que são determinadas possuem duas possibilidades de recuperação: total ou parcial, dependendo do problema identificado. No caso Total, é preciso que seja realizada uma reinstalação em todo o sistema (operacional, rede, aplicação). Ela ocorre quando existem falhas físicas de hardware ou corrompimento do sistema operacional. No caso da Parcial, ela é caracterizada pela perda parcial de informações, no qual é possível restaurar o que foi danificado. Suas causas são, por exemplo, arquivos apagados por engano e atualizações de sistema que corrompem bancos de dados.

As estratégias de continuidade são descritas em quatro características: Cold (baixo custo e backup dos dados envolvidos no serviço); Warm (e backup dos dados e snap-shot dos servidores envolvidos no serviço); Hot (equipamento/espaço reservado próprio, locado ou cedido, onde são feitas atualizações constantes do serviço e dados relacionados); e, por fim, Mirrored (atualizações de sistemas e dados em tempo real).

Assim, a manutenção é caracterizada pela validação e atualização de toda a documentação criada para que os procedimentos e as informações possibilitem à empresa continuar seus processos críticos, mesmo que haja algum tipo de interrupção neles.

6 Como implantar e gerenciar os OKRs

Os OKRs (objectives and key results), ou objetivos e chaves de resultados, têm uma estrutura simples e objetiva, que foca a estratégia, unindo as equipes. A sigla corresponde a:

- Objectives (objetivo): objetivos claros do que a empresa quer conquistar.
- Key Results (chave de resultados): são os parâmetros que determinam o quanto a empresa está perto de alcançar os resultados definidos por ela.

Sua estruturação envolve metas claras e específicas, objetivos definidos pela equipe, estabelecimento de prazos curtos, acompanhamento constante dos resultados e divulgação dos OKRs para os colaboradores, assim todos estarão trabalhando por algo em conjunto. É preciso estabelecer a situação atual da empresa, onde se quer chegar (conquistar), o que deve ser mudado ou melhorado para que os objetivos sejam alcançados, como serão as melhorias e como serão medidas essas conquistas (mensurar o progresso).

Para implementação do OKR na empresa, são seguidos os seguintes passos:

1. Formulação da estratégia: deve-se analisar junto aos gestores da organização quais serão os objetivos a serem alcançados anualmente ou mesmo em prazos menores.

2. Envolvimento e treinamento da equipe: os funcionários devem estar cientes dos objetivos da organização, do que se espera deles para o atingimento das metas e serem treinados para as atividades a serem executadas.

3. Implantando o OKR gradualmente: iniciando com um projeto-piloto, nos níveis superiores da empresa, primeiramente. Assim, é possível observar os problemas de forma menos impactante para todos os níveis da organização.

4. Prepare a empresa para os OKRs: é importante ter bem claro quais serão os OKRs definidos pela empresa, e podem ser necessários alguns encontros com os especialistas de OKR de dentro da organização ou mesmo consultores externos. Se não for possível reunir todos os colaboradores, é essencial garantir que os gestores estejam presentes.

5. Definição dos OKRs: o prazo mais comum para os OKRs é de 3 meses, projetando, executando e avaliando continuamente. O

processo pode ser top-down (de cima para baixo) ou bottom-up (de baixo para cima) em relação aos níveis da organização.

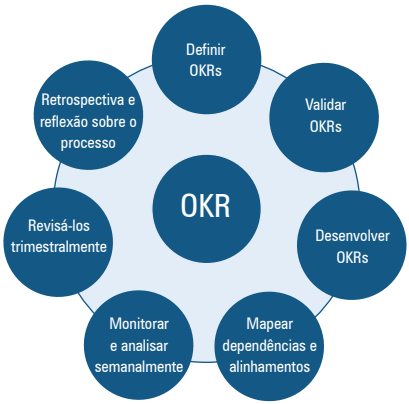
6. Ciclos: os ciclos de OKR dependem de cada organização, porém, é importante o acompanhamento semanal, para realizar os ajustes necessários.

7. Classificação: classificam-se os resultados de OKR, numa escala de 01 a 10.

Para a implantação do processo, uma mudança de cultura é necessária, pois os OKRs devem fazer parte do dia a dia dos líderes e colaboradores, para realização de todas as etapas do planejamento.

A figura 2 a seguir demonstra o passo a passo do funcionamento dos OKRs:

Figura 2 – Funcionamento OKRs



Considerações finais

Finalizando este capítulo, chegamos ao ponto essencial de que as organizações devem centrar esforços não somente na sua concorrência, produtos, serviços e clientes, mas também elaborar um plano de continuidade de seus negócios, com uma visão estratégica do negócio.

Vimos que analisar os processos de continuidade dos negócios é uma parte muito importante para auxiliar a empresa a lidar com diferentes situações e variados níveis de gravidade. A instituição passa por diversos desafios e precisa saber como vai proceder desde a identificação do problema.

Dois processos compõem esse mecanismo de defesa: o BIA e os OKRs. Vimos que o BIA define parâmetros que envolvem prazos para recuperação e os gastos envolvidos nos processos, além de identificar os processos fundamentais que garantem a sobrevivência da organização. Já os OKRs definem as estratégias e tarefas que cada equipe vai executar dentro da empresa para alcançar os resultados almejados por ela.

Atualmente, com o grande acesso a informações, os ataques se tornam mais constantes e perigosos. As empresas devem utilizar os recursos efetivos disponíveis para preservação ou eventuais impactos que podem acometê-la. É preciso pensar no presente e projetar o futuro para que as consequências sejam as mais brandas possíveis.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 22301:2020**: Segurança e resiliência – Sistema de gestão de continuidade de negócios. Rio de Janeiro: ABNT, 2020.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR 15999-1: 2007**: Gestão de Continuidade de Negócios. Rio de Janeiro: ABNT, 2007.

ALMEIDA, A. P. **Boas práticas de gestão de serviços de TI com o uso de ferramentas automatizadas no gerenciamento de ativos**. Santa Catarina: Unisul, 2018. Disponível em: https://repositorio.animaeducacao.com.br/bitstream/ANIMA/4022/1/Artigo%20Cientifico%20-%20Anderson%20Paiva%20de%20Almeida.pdf. Acesso em: 10 set. 2021.

BAARS, H. et al. **Fundamentos de segurança da informação**: com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018.

DUPONT, M. **Plano de continuidade de serviços de TI**: implantação e manutenção de infraestrutura. Porto Alegre: Conselho Regional de Engenharia e Agronomia do Rio Grande do Sul, 2018. Disponível em: http://saturno.crea-rs.org.br/pop/info/POP/Plano%20de%20Continuidade%20de%20Servi%C3%A7o.pdf. Acesso em: 10 set. 2021.

FRIEDENHAIN, Vitor. **Um estudo sobre métodos e processos para implantação da gestão de continuidade de negócios aplicáveis a órgãos da administração pública federal brasileira**. 2008. Monografia de Especialização (Departamento de Ciência da Computação) – Universidade de Brasília, Brasília, 2008. Disponível em https://dsic.planalto.gov.br/cegsic/83-monografias-da-1-turma-do-cegsic. Acesso em: 21 ago. 2021.

INSTITUTO FEDERAL DE SANTA CATARINA. **Sistema de Gestão de Continuidade de Negócios de Tecnologia da Informação e Comunicação SGCN – TIC**. 2018. Disponível em: https://www.ifsc.edu.br/documents/526028/877206/istema+de+Gest%C3%A3o+de+Continuidade+de+Neg%C3%B3cios+de+TI+do+IFSC.pdf/f8680616-60be-9a03-3f9d-28159ebe5ab6. Acesso em: 4 jun. 2021.

IWASA, Fabio Takeji; TAVARES, Elaine. Fatores críticos para a qualidade de serviço em TI: uma análise a partir do modelo SERVQUAL. In: CONGRESSO DE GESTÃO, NEGÓCIOS E TECNOLOGIA DA INFORMAÇÃO – CONGENTI, 1., 2017. Rio de Janeiro. **Anais**... Rio de Janeiro: Ebape/FGV-RJ, 2017. p. 1-23. Disponível em: https://eventos.set.edu.br/congenti/article/viewFile/7955/2910. Acesso em: 14 set. 2021.

PRIMÃO, A. P. **Sistema de gestão de continuidade de negócios de tecnologia da informação e comunicação**. Florianópolis: Instituto Federal De Educação, Ciência e Tecnologia de Santa Catarina, 2018.