Capítulo 8

Plano de contingência

Conforme já abordado em capítulos anteriores, a segurança da informação se determina pelo resguardo da confidencialidade (informações acessíveis somente aos responsáveis), integridade (proteção de informações e métodos de como realizá-la de forma efetiva), e, por fim, disponibilidade (garantir que pessoas autorizadas acessem ativos e informações de forma segura) (BAARS et al., 2018). Portanto, a informação é um dos ativos fundamentais para que uma empresa sobreviva e seja bem-sucedida. Entender a importância que esses dados fazem para a instituição e sua segurança faz com que se busquem formas de permanecer no mercado de maneira segura e constante.

As falhas que podem acometer os sistemas de uma empresa impactam diretamente e significativamente seu funcionamento. Esses erros podem ser oriundos de falha humana, ataques internos, externos e

físicos, como quedas de energia, além de naturais, como enchentes ou incêndios.

Empresas preparadas para lidar com essas questões, conseguem recuperar-se de maneira efetiva para não afetar a dinâmica da companhia e evitar problemas mais graves.

O preparo para essas situações está ligado diretamente ao quesito prevenção ou contenção de problemas. Para isso, é fundamental ter um plano de contingência que assegure a continuidade dos serviços de TI, mesmo em momentos de indisponibilidade do sistema, e que apoie a importância de estabelecer medidas técnicas e procedimentos completos que permitem que um serviço de TI ou um conjunto de serviços sejam recuperados de forma rápida e positiva após uma interrupção ou cenário de desastre.

Este capítulo visa abranger fundamentos que norteiam planos de contingência, como estratégias para prevenir problemas que possam desestabilizar a empresa, análise de impacto e protocolos que possibilitam continuidade nos negócios, mesmo em momentos com efeitos negativos, além de entender as responsabilidades de cada membro da equipe em momentos delicados como esses.

1 Fundamentos sobre plano de contingência

Um plano de contingência é um curso de ação projetado para ajudar uma organização a responder com eficácia a um evento ou situação futura significativa que pode ou não acontecer. De acordo com Andrade et al. (2011), faz-se importante adotar um plano de contingenciamento não só em razão dos equipamentos e processos em tecnologia da informação serem falhos como também pelo fato de estarem sujeitos a inúmeros riscos dentro ou fora da organização.

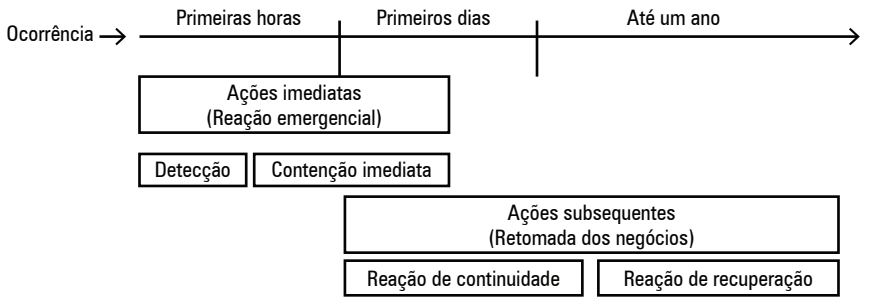
Portanto, para estar preparado para impactos que podem ou não acontecer na instituição, a prevenção é a melhor estratégia.

Dentre os fundamentos que devem ser considerados, temos:

- Cenários: simulações de diversos cenários com diferentes níveis de riscos, como uma queda de energia ou ataques hackers.
- Gatilhos: cada ação delineada no plano de contingência irá "ligar o alerta" da empresa, ou seja, acionar gatilhos.
- Resposta: uma breve descrição da estratégia a ser adotada para a resposta ao evento que possa ocorrer.
- Quem informar: identificação sobre as pessoas que precisam saber o que acontece em cada incidente, inclusive considerando as autoridades competentes.
- Responsabilidades definidas: atribuição das responsabilidades para os(as) funcionários(as) envolvidos(as).
- Linha do tempo: definição de ações a serem executadas em períodos definidos de tempo, como: informar toda a equipe sobre o problema X nas primeiras 12 horas após o evento acontecer.

A figura 1 a seguir mostra de forma dinâmica a cronologia da ocorrência e as providências que precisam ser tomadas durante o processo.

Figura 1 – Cronologia



Fonte: adaptado de QSP (2017).

Na situação de uma ocorrência que ameace a segurança das informações, a equipe responsável pelo plano de contingência precisa estabelecer prioridades. É importante que nas primeiras horas, conforme ilustrado na figura 1, as intercorrências sejam mitigadas, ou seja, detectadas e contidas de forma rápida e eficaz, sem haver impacto no funcionamento da empresa. Após os passos iniciais serem colocados em prática e o negócio retomado sem maiores riscos, a equipe deve estabelecer a continuidade, isto é, a empresa seguirá resolvendo o problema, porém, seu funcionamento prosseguirá de forma que não prejudique a dinâmica da organização. Por fim, a reação de recuperação consiste no retorno na recuperação e planejamento para que os processos melhorem e salvaguardem os negócios em possíveis novas ocorrências.

PARA SABER MAIS

Para aprofundar seus conhecimentos sobre o plano de contingência, consulte o livro *Gerenciamento de projetos: guia do profissional – fundamentos técnicos*, de Dalton Louzada et al. (2006).

2 Política de contingência

A política de contingência se define por um planejamento de sistemas preventivos que asseguram a continuidade dos sistemas essenciais à empresa em momentos de crise. O início do plano de contingência deve conter uma política clara sobre as definições dos objetivos das contingências. A alta administração e a direção de TI devem estar presentes no desenvolvimento da política. Os principais elementos políticos são:

- Responsabilidades de cada setor – cada equipe deve saber suas responsabilidades e como prevenir e lidar com as ameaças. Neste tópico, temos equipes como comitê de desastres

(acompanhamento de ocorrências); equipe de ambientes, as quais são responsáveis pelas instalações físicas; equipe de redes, que identifica danos na infraestrutura de rede; equipe de servidores, que garante que as aplicações essenciais da empresa continuem a funcionar mesmo em meio à crise; equipe de comunicação, responsável por todas as comunicações realizadas durante o momento de impacto; equipe de backup, que, como o próprio nome já diz, é responsável pelos armazenamentos e por quantificar dados perdidos e tempo de recuperação; e, por fim, a equipe de segurança da informação, responsável por prover mecanismos de segurança em aplicações e dados.

- Âmbito das áreas contempladas no planejamento de contingência: ou seja, as áreas de ambientes, redes, servidores, comunicação backup e segurança.

- Recursos necessários: para que seja possível realizar um plano de contingência efetivo, é preciso estabelecer o cenário, contar com as equipes descritas acima, cada uma com sua responsabilidade, equipamentos preparados para crises (backup), e definir formulários, checklists e relatórios que auxiliem na execução da contingência.

- Requisitos de formação: os responsáveis devem ter formação compatível com as demandas solicitadas em momentos de contingência, relacionadas a sistemas, infraestrutura e relacionais.

- Agenda de testes: como parte do plano de contingência, as informações coletadas em momentos de crise são importantes para definição das ações e como executá-las de maneira que não prejudiquem a empresa e possibilitem sua continuidade nos negócios.

- Planejamento de cronograma de manutenção: cada empresa estabelece um cronograma de testes para verificar seu plano de contingência (equipes, equipamentos), identificar possíveis falhas e reparar o que for necessário.

- Frequência de backups e armazenamento de mídia de backup: como o próprio nome já diz, o backup garante à empresa segurança de seus dados em momentos de falha e garantem segurança no seu segmento.

O conjunto de todos esses elementos garante uma boa execução do plano de continuidade dos negócios e possibilita que a empresa continue a execução de seus processos.

PARA SABER MAIS

Para aprofundar seus conhecimentos acerca da política de contingência, conheça o livro *Políticas e normas para a segurança da informação*, do autor Edison Fontes (2012).

3 Realizar a análise de impacto do negócio (BIA)

Como vimos em capítulos anteriores, a análise de impacto do negócio (BIA) é um processo essencial que permite que a empresa caracterize completamente os requisitos, os processos e as interdependências dos sistemas e serviços, utilizando essas informações para determinar os requisitos e as prioridades de contingência.

Será realizada, então, uma correlação de todos esses elementos descritos acima e, assim, com base nesses dados, teremos caracterizadas as consequências de uma interrupção do sistema, por exemplo. Os resultados do BIA são, portanto, incluídos nas estratégias do plano de continuidade e recuperação da empresa.

4 Identificar os controles e as medidas preventivas

Saber identificar o que é vital para a sobrevivência de uma empresa possibilita que sejam identificados pontos cruciais que devem ser cuidados em questão de segurança. Os impactos de incidentes podem ser eliminados através de medidas preventivas, cujo objetivo é afastar, detectar e reduzir esses impactos (MARTINS, 2014). As estratégias de continuidade devem minimizar ao máximo os riscos e impactos negativos que possam acometer a organização. O que deve ser analisado com cautela é a viabilidade operacional e financeira, pois é fato que o método preventivo é melhor que ter de recuperar um sistema ou serviço após uma interrupção (FONTES, 2012).

Uma maneira de se controlar os impactos que uma empresa pode sofrer é por meio da informação, a começar por seus colaboradores, os quais precisam ser frequentemente atualizados e instruídos dos procedimentos de segurança referente às suas atividades e backups. Além disso, a empresa deve ter suporte técnico (equipes de rede, servidores, comunicação e backup) para tratar preventiva ou efetivamente em momentos de crise, como já determinado anteriormente.

Os métodos de tratamento precisam estar em coerência com a ISO 27000, a qual trabalha com os três pilares já mencionados neste capítulo: integridade, disponibilidade e confidencialidade. Para Martins (2014), o ponto de partida para a implantação de um plano de contingência é a definição dos papéis e das responsabilidades de cada um na instituição, sendo sempre supervisionados pela equipe gestora, que deve colaborar de maneira direta e ativa no planejamento e na preparação dos colaboradores. Sendo assim, o projeto deve abranger quatro momentos: 1. análise (atualização de planos de contingência); 2. planejamento (escopo, equipes, projeto e cronograma); 3. desenvolvimento (estratégias BIA); e 4. checagem (testes, simulações, identificação de

falhas, emissão de relatórios) (MARTINS, 2014). Martins (2014) ainda menciona que o monitoramento dos riscos é um processo contínuo, cujo objetivo é a prevenção de possíveis ameaças e mitigação de forma objetiva e rápida. Esses métodos devem estar presentes no plano de contingências aqui estudado.

5 Estratégias para recuperação dos negócios

Após identificação pela análise de impacto de negócios (BIA), o(a) profissional de TI deve elaborar estratégias de recuperação efetivas para as situações que possam ocorrer que interrompam um serviço da organização. A recuperação envolve equipes de segurança responsáveis, gestores da empresa e funcionários. Cada um tem seu papel definido (recuperação de dados e/ou infraestrutura) para colocarem a empresa em funcionamento novamente.

Deve ser levado em consideração:

- Custos: identificar o quanto a empresa perderia diante da indisponibilidade e investimento em recuperação dos riscos.
- Tempo de interrupção permitida: mensurar o quanto a empresa perderia financeiramente e em credibilidade/imagem por estar fora de funcionamento.
- Segurança: como lidar com possíveis perdas e recuperação de sistema.
- Integração com todo o plano de contingência: trabalho com todas as equipes para resolver de forma breve e efetiva a crise em que a empresa se encontra.

Todos os tópicos mencionados acima são importantes diante do quadro que será estabelecido no momento de definição das estratégias para lidar com o problema encontrado.

6 Realizar testes do plano de contingência

Colocar o plano de contingências em prática, na forma de testes, é uma etapa importante do plano em si, pois permite que os problemas sejam identificados e consequentes ajustes de procedimentos sejam discutidos entre a equipe responsável.

Os problemas que podem acometer uma empresa são diversos (perda de serviços de TI, indisponibilidade ou perda de energia elétrica, alagamento, incêndio, desmoronamento, greves, congestionamentos e indisponibilidade de serviços, hackers, falhas de sistema etc.). Todas as questões colocadas aqui impactam o dia a dia da empresa e podem atrasar seus processos, impactando diretamente seu funcionamento.

Para lidar com essas questões, os testes analisam os impactos que serão causados em diversas situações. As equipes responsáveis identificam o problema (com base em um cenário de crise) e trabalham de forma que contemplem os quatro pilares: analisar, planejar, desenvolver e checar, considerando recursos mínimos necessários para dar continuidade às atividades, quais atividades serão contidas e quais as prioridades para o restabelecimento. Após passar por todos os processos, a emissão de um relatório e de checklists auxilia na definição da falha, elaboração de estratégias para restaurar os problemas e melhorar o plano de contingência da empresa de modo a não haver prejuízos maiores em um momento de crise. A figura 2 a seguir ilustra como processo é realizado:

Figura 2 – Processo de realização do plano de contingência e continuidade do negócio

Os testes auxiliam na prevenção de falhas que a empresa pode apresentar em um momento de crise. Portanto, são de extrema importância para anteciparem os riscos e como tratá-los diante das adversidades.

7 Treinamento das equipes envolvidas

A equipe envolvida nos procedimentos do plano de contingência deve executar os testes e avaliá-los quanto à capacidade da própria equipe de executar todos os processos para todos os casos. Assim, a alta administração pode avaliar se a equipe deve ter novos integrantes ou mesmo efetivar a contratação de uma consultoria especializada.

Em conformidade com o que já foi citado no capítulo, o envolvimento das equipes é essencial para o bom desenvolvimento do plano de contingência. Cada uma delas é responsável por um processo que definirá os próximos passos para o restabelecimento seguro das atividades realizadas na organização.

Os papéis e as responsabilidades de cada um são acionados diante de um desastre. As equipes são formadas por colaboradores que são constantemente atualizados e treinados para situações ou, quando necessário, por meio da contratação de equipes externas especializadas. A equipe de recuperação define qual foi a questão encontrada e quais serão os próximos passos (definição da ameaça e como será tratada). Ela é composta por autoridades no nível institucional. A equipe de instalações e ambientes são responsáveis pelas instalações físicas dos sistemas de TI. Eles avaliam os danos e determinam as reparações, quando necessárias. A equipe de rede avalia danos na estrutura de rede e transmissão da empresa, e também repara quando algo necessita ser melhorado. A equipe de servidores apoia a equipe de TI de forma física e virtual para conseguirem continuar operando em momentos de crise. A equipe de comunicação é responsável por estabelecer e manter a comunicação entre funcionários, clientes, autoridades e fornecedores. As equipes de backup e segurança da informação resguardam informações e dados importantes diante de uma crise.

Para Martins (2014), as equipes são treinadas focando na avaliação do risco e controle dele, análise do impacto no negócio (BIA), estratégias para continuidade (auditoria, manutenção), preparação e resposta em caso de crises e ameaças, além de programas de conscientização e orientação de segurança, comunicação em momentos de crise e coordenação com agências externas.

Cada equipe é responsável por um processo e pela execução do mesmo. Cada colaborador é peça-chave no sucesso do plano, no restabelecimento das atividades e no bom curso da empresa.

Considerações finais

Conforme vimos neste capítulo, o plano de contingência de TI é fundamental para que as organizações possam atuar de forma ideal, evitando problemas com prejuízos por alguns momentos de inatividade do negócio.

As empresas precisam estar cientes de todos os processos que podem acontecer e que levarão a riscos para a continuidade de seu funcionamento. A análise de impacto auxilia diretamente a entender o que seria prejudicial à empresa e o que deveria ser melhorado em seus processos.

As equipes que compõem um plano de contingência são treinadas para atender a instituição quando necessário. Cada uma delas é responsável por sua parte, mas com um objetivo comum: a continuação ou o restabelecimento das atividades da empresa.

Ao analisar os impactos que fatores diversos podem acometer as atividades, é possível traçar planos preventivos para evitar que falhas aconteçam. Identificar essas falhas e criar estratégias em um momento de teste é crucial para que a empresa consiga lidar com desafios e continue no mercado de forma confiável e segura.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27000** – Tecnologia da Informação – Técnicas de Segurança – Código de prática para gestão da segurança da Informação. Rio de Janeiro: ABNT, 2006.

ANDRADE, Daniel et al. **Plano de contingência de ti**: preparando sua empresa para reagir a desastres e manter a continuidade do negócio, 2011. Dissertação (Pós-Graduação em Segurança da Informação) – Faculdade Senac/DF, Brasília, 2011.

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

FONTES, E. **Políticas e normas para a segurança da informação**. Rio de Janeiro: Brasport, 2012.

LOUZADA, Dalton et al. **Gerenciamento de projetos**: guia do profissional – fundamentos técnicos. Rio de Janeiro: Brasport, 2006.

MARTINS, R. **Gestão da continuidade de negócios** – análise de impacto de negócio para entidades fechadas de previdência complementar (EFPC). 2014. Trabalho de conclusão de curso (Graduação em Redes de Computadores) – Centro Universitário de Brasília: Instituto CEUB de Pesquisa e Desenvolvimento – ICPD, Brasília, 2014.

QSP. **Planejamento de contingências**. 2017. Disponível em: https://www.qsp.org.br/pdf/GCN_conforme4360.pdf. Acesso em: 1 jul. 2021.

SETIM – Secretaria de Tecnologia da Informação e Modernização. **Plano de Continuidade de TI**. Salvador: Tribunal de Justiça da Bahia, 2018.

Sobre o autor

Márcio Guimarães Konopczyk é graduado em administração de empresas com MBA em gestão de finanças corporativas. Atua na área de TI desde 1976, tendo participado de todos os processos evolutivos da área de informática. Tem experiência como programador de computador Cobol, analista de sistemas e coordenador de projetos de sistemas, tendo atuado em diversas empresas, como Olympia do Brasil, Interclínicas, Enterpa S.A., Araújo Engenharia e Grupo Dedini. Em 1988 iniciou suas atividades como consultor técnico na área de informática, participando de centenas de projetos de desenvolvimento de sistemas, auditorias, consultoria empresarial, financeira, operacional e de TI. Professor eventual do Senac na área de desenvolvimento de sistemas, palestrante de Business Intelligence, auditoria de sistemas e oratória. Desenvolveu inúmeros trabalhos sobre análise preditiva, auditoria de sistemas, gestão de segurança da informação e gestão de projetos dos mais variados segmentos e indicadores de desempenho. Desde 2002, concentra seus trabalhos como consultor corporativo auxiliando no desenvolvimento de muitas empresas nos mais variados segmentos de mercado.