NetSupport

Como montar um plano de gestão de crise para a área de TI

SUMÁRIO

Quando se fala em gestão, tecnologia e investimentos em geral, é essencial estar preparado para todos os tipos de cenário que podem acometer uma empresa. Muitos gestores, por estarem com seu negócio em ascensão, acabam não pensando muito sobre os **planos de contingência** para momentos de crise e incerteza. Ninguém tem a situação sob controle o tempo todo, e acontecimentos imprevisíveis, tanto internos quanto externos, podem ser a causa de **danos irreversíveis** para aqueles que não estão preparados.

A TI, ao assumir um papel estratégico dentro das corporações, acaba exigindo um **planejamento emergencial**, um conjunto de ações previamente calculadas que possam mitigar efeitos negativos ou até mesmo eliminá-los. A prevenção é o que deve orientar esse processo de organização, que não pode esperar a boa vontade do gestor. Ele deve estar pronto o quanto antes. Com este e-book, você terá todo o material necessário para começar a montar seu plano de gestão de crise agora. Você vai ver:

- O que é o plano de gestão de crise?
- Importância do plano de gestão de crise
- Como elaborar um plano de gestão de crise para TI
- 7 dicas para não errar na gestão de crise

Boa leitura!

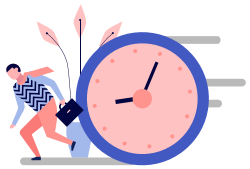
O que é o plano de gestão de crise?

O plano de gestão de crise é um guia elaborado pela empresa, unindo todas as **orientações necessárias para que os setores tenham uma metodologia de trabalho durante o enfrentamento de situações inesperadas.**

Essas situações compreendem crises econômicas, problemas ambientais, incêndios, contaminação de produtos, disputas trabalhistas, corrupção, desastres da natureza e quaisquer outras que possam trazer prejuízos significativos ao negócio. É preciso pensar nele com o máximo de antecedência possível, visto que uma empresa despreparada, quando se vê no meio de uma crise, acaba sofrendo perdas com uma velocidade e uma intensidade muito maiores.

Com o plano de gestão de crise, é possível ganhar tempo, manter as operações em funcionamento e passar pela situação com alguma estabilidade. Em momentos de crise, a preocupação não é estar com alto nível de produtividade e lucro, mas sim sobreviver e manter a empresa erguida. Quem é responsável por uma organização sabe que essa, por si só, já uma tarefa bastante desafiadora.

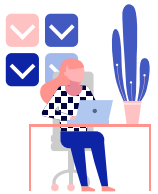
Para fazer com que o plano de contingência tenha êxito, a empresa de forma geral deve cumprir alguns requisitos básicos. São eles:



Agilidade para colocar o guia em prática;

Tranquilidade, pois um momento de crise é sinônimo de situação desfavorável e, quando administrado de forma impulsiva e precipitada, pode trazer prejuízos ainda maiores;

Versatilidade, pensando que a equipe disponível e os recursos no momento da crise possam ser diferentes que o planejado, encontrando maneiras de ajustar o protocolo de forma a manter a produtividade;



Capacidade de avaliar situações de crise e aprender com elas, tirando o máximo de lições da crise e impedindo que os mesmos erros sejam cometidos no futuro.

Importância do plano de gestão de crise

Como já dito, o principal objetivo do plano de gestão de crise é blindar a empresa em momentos difíceis, impedindo e evitando perdas muito graves.

Porém, a parte financeira do negócio não é a única razão para começar agora um plano de ação. Esse planejamento permite uma ação muito mais rápida e eficaz em outras áreas. Pensando no setor de TI, por exemplo, uma crise interna provocada por **ataques virtuais** no servidor pode ser sanada com agilidade, evitando que dados importantes do negócio sejam perdidos ou vazados.

Durante uma crise financeira ou de saúde pública, como a provocada pela COVID-19 em 2020, **a tecnologia pode ser uma forma de manter as operações da empresa em funcionamento e com um gasto mais reduzido**, com os colaboradores atuando remotamente.

Para isso, é claro, é necessário um planejamento prévio de toda a **infraestrutura de TI** necessária para que a proposta se concretize.

Além disso, em casos de problemas que comprometam a imagem da empresa com o público externo, como escândalos, falhas graves na prestação de serviços ou com a qualidade de produtos, a empresa que toma medidas rápidas consegue também **restabelecer sua imagem mais facilmente**.

Simplificando, podemos dizer que a importância da gestão de crise está em:

- **Diminuir o impacto do ocorrido interna e externamente;**
- **Auxiliar na tomada de ação rápida e eficaz;**
- **Preservar a imagem da empresa no mercado;**
- **Evitar que problemas semelhantes se repitam;**
- **Transmitir compromisso com a sociedade e outros empresários parceiros;**
- **Garantir o alinhamento e preparo das equipes de trabalho;**
- **Blindar o negócio, garantindo sua sobrevivência.**

Como elaborar um plano de gestão de crise para TI

Como vimos até aqui, o plano de gestão de crise é essencial para qualquer empresa. Considerando que o setor de TI exerce **funções estratégicas e operacionais** em uma organização, ter um guia que oriente sua atuação em situações de crise é essencial.

Vejamos o passo a passo da construção de uma estratégia segura em torno dos riscos do setor:

1. Defina o escopo

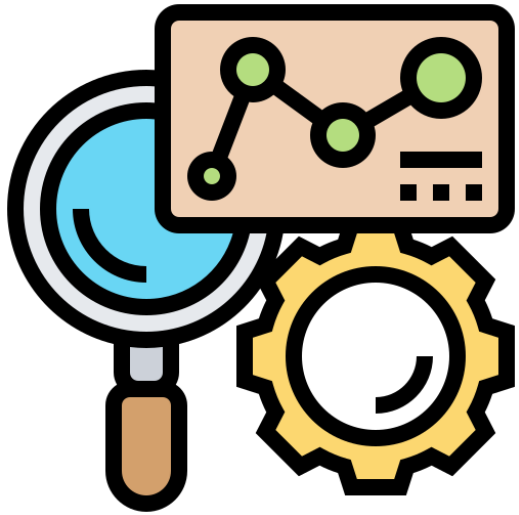
Todo o processo de construção do plano de gestão de crise será condicionado aos riscos aos quais o setor de TI está sujeito. O primeiro passo é **definir quais desses riscos serão considerados**, tendo um escopo mais claro.
Serão riscos de um projeto específico? Dos processos operacionais do setor? Do planejamento estratégico?

2. Faça um brainstorming com a equipe

Levantar informações, fazer anotações e ouvir os profissionais do setor é muito importante para começar a traçar um guia eficiente. Faça um brainstorming com os colaboradores e pergunte que cenários negativos elas conseguem imaginar e o que pode ser feito em cada um deles.

Afinal, caso uma crise realmente se torne um problema, todos deverão atuar de forma conjunta, unindo forças para que o planejamento dê certo. Assim, com a participação de todos desde a criação do protocolo, as chances do engajamento ser mais efetivo é muito maior.

3. Faça o diagnóstico de riscos



A identificação dos riscos é uma etapa mais do que importante. É nela que a equipe de TI identifica contra o que estará lutando. Para conseguir definir os riscos com mais assertividade, **pense sobre possíveis eventos e cenários reais que você consegue visualizar no contexto da sua empresa.** Lembre-se de ser o mais específico possível nas respostas a esse tópico. Projeções vagas não serão úteis quando o plano de gestão de crise for realmente necessário.

4. Identifique os controles de cada risco

Os chamados controles de risco são as atividades, procedimentos ou mecanismos que, se implementados, podem agir sobre um risco; são **ações que trabalham de forma a reduzir o impacto negativo para o setor.**

5. Atribua uma probabilidade

Definidos os riscos, é útil também **determinar o nível de probabilidade** de cada um deles. A escala utilizada pode variar de 0 a 10, por exemplo, ou ser classificada como alto, médio e baixo risco. A escolha varia de acordo com as necessidades de cada negócio.

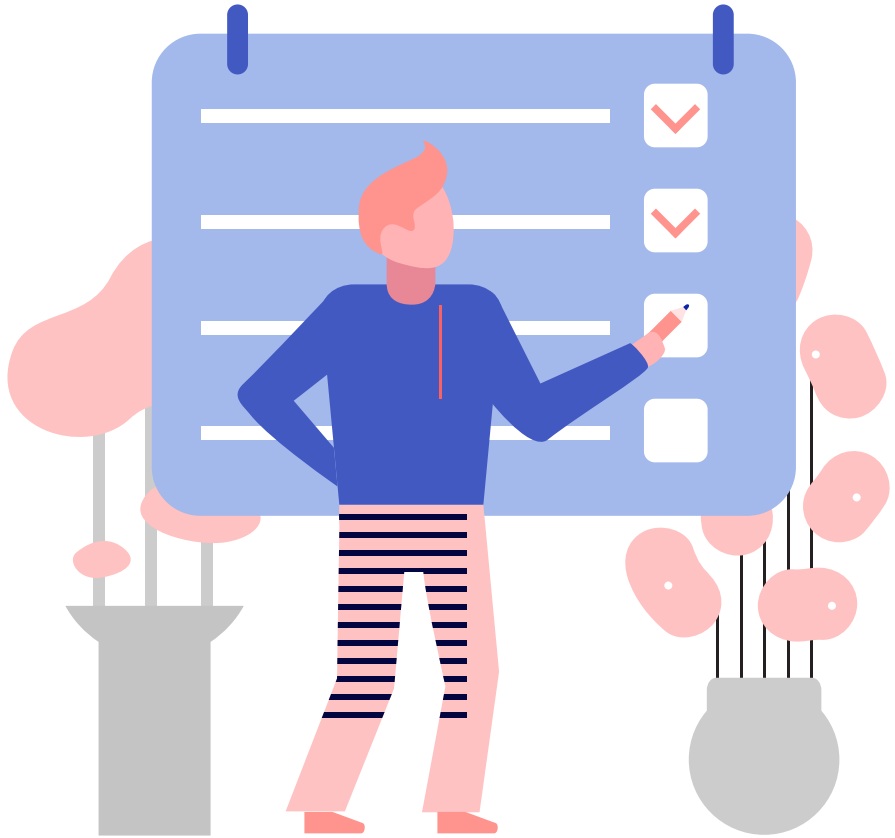
6. Visualize o impacto

O próximo passo é definir o impacto de cada risco, ou seja, **o quanto cada cenário pode ser prejudicial para o negócio**. Assim como na etapa de probabilidade, o impacto pode ser considerado em níveis ou escala numérica.

7. Defina prioridades

Ao chegar nesta etapa, você já terá em mãos um conjunto de cenários de risco para o setor, assim como as probabilidades de se tornarem reais, os impactos que podem causar e quais as ações disponíveis para lutar em cada um deles.

Sabemos que o ideal é que nenhuma das possibilidades se torne realidade, mas como é impossível dar conta de tudo ao mesmo tempo, o ideal é definir prioridades, **ordenando os riscos por meio de uma lista**, por exemplo. Identifique os riscos mais críticos e os menos críticos.



8. Elabore um plano de mitigação e um de contingência

Tendo todas as informações dos tópicos anteriores em mãos, você saberá quais as situações que podem ocasionar uma crise nos processos do seu setor de TI. Nesse ponto, temos duas considerações importantes:

Estratégia de mitigação

Um plano de ação que busca reduzir a probabilidade de um risco se tornar realidade. Isso significa definir o que pode ser feito agora para evitar que no futuro os prejuízos sejam maiores.

Estratégia de contingência

Um planejamento focado em pensar para além da prevenção, visualizando ações que deverão ser tomadas em caso de alguma falha. Isso possibilita que a gestão já saiba imediatamente o que fazer, economizando tempo e reduzindo o prejuízo.

9. Realize uma auditoria e aplique as estratégias de mitigação

Agora é o momento de começar a colocar em prática um pouco do que foi planejado. Tendo as estratégias de mitigação bem definidas para cada um dos riscos, é fundamental promover uma auditoria por todo o setor de TI.
A partir disso, será possível **identificar possíveis brechas nos processos**, aplicando o quando antes as ações preventivas.

10. Avalie o desempenho das ações

Após realizar a auditoria e aplicar as ações de mitigação, é necessário verificar se realmente houve uma otimização, ou seja, se tudo está funcionando melhor após as alterações.

Através disso, a gestão terá uma **análise do quão eficazes são as estratégias propostas** e concluir se é necessário ou não fazer alguma alteração.

11. Refaça os cálculos de riscos

Depois dessa primeira análise de resultados, caso tenha obtido dados positivos, logicamente o nível de probabilidade dos riscos terá diminuído. Faça o cálculo de risco residual e **confira se ainda está preocupante ou se passou para um nível aceitável**, por exemplo.

12. Monitore constantemente

Se engana quem pensa que o planejamento de gestão de crise é uma tarefa que pode ser deixada de lado após algumas etapas cumpridas. O monitoramento deve ser constante. Uma boa dica é investir em **softwares de monitoramento** que verificam a qualidade de toda a infraestrutura utilizada por sua empresa.

Isso significa **ter um diagnóstico frequente da qualidade das redes e da performance de máquinas**, além de contar com o envio de alertas para o administrador dos sistemas em caso de identificação de anomalias, por exemplo.

Esse é um tipo de investimento inteligente que evita gastos maiores no futuro. Seguindo o plano de gestão de crise, a equipe saberá o momento de tomar providências mesmo antes da chegada de problemas maiores.

Para não esquecer!

- [ ] Defina o escopo
- [ ] Faça um brainstorming com a equipe
- [ ] Faça o diagnóstico de riscos
- [ ] Identifique os controles de cada risco
- [ ] Atribua uma probabilidade
- [ ] Visualize o impacto
- [ ] Defina prioridades
- [ ] Elabore um plano de mitigação e um de contingência
- [ ] Realize uma auditoria e aplique as estratégias de mitigação
- [ ] Avalie o desempenho das ações
- [ ] Refaça os cálculos de riscos
- [ ] Monitore constantemente

7 dicas para não errar na gestão de crise

Mais do que seguir o passo a passo mostrado no tópico anterior, a gestão deve estar ciente de que isso não é tudo. Toda a construção de uma estrutura segura para que a empresa possa seguir em tempos de crise depende de um *conjunto de elementos* que devem estar presentes na cultura organizacional dela. Alguns dos *aspectos essenciais* que podemos destacar são:

1. Organize a equipe

Para que o planejamento realizado para uma gestão de crise efetiva mostre os resultados esperados, é importante que a equipe de TI esteja muito bem organizada. Em outras palavras, **cada componente deve ter clareza quanto a seu papel no processo, assim como um líder bem definido.**

Em momentos de incerteza, onde a responsabilidade e a pressão por ações assertivas aumentam, é inaceitável que haja espaço para insegurança no time.

2. Proponha um plano detalhado

Em cenários de crise, é preciso que o time de TI tenha consciência de tudo que será feito. É preciso ter a clareza para entender o contexto e buscar soluções. Por isso, o plano de gestão de crise deve ser **o mais detalhado possível** e, acima de tudo, de **fácil compreensão**. Daí a importância de dar ao processo a devida atenção, imaginando todos os tipos de problema pelos quais o setor de TI pode passar e como manter as operações mais importantes em funcionamento em qualquer uma delas.

Isso significa não ter medo de assumir a pior possibilidade, seja em termos financeiros, legais ou de **segurança da informação**, por exemplo.Para exemplificar, busque incluir o máximo de indicadores de TI úteis, como:

Recovery Time Objective (RTO): responsável por indicar em quanto tempo o sistema pode ficar parado aguardando restauração, definindo um tempo máximo em que deve ser restaurado após uma falha para que não haja consequências graves;

Recovery Point Objective (RPO): que corresponde ao volume de dados perdidos nos casos de tempo de inatividade do serviço.

3. Realize testes

O plano de gestão de crise não deve ser feito por obrigação e ser deixado de lado após algum tempo. Quando ele se torna desatualizado ou não tem sua eficácia comprovada, ele acaba não servindo de nada em um momento realmente crítico.

Se você não quer que sua equipe de TI fique na mão quando algo der realmente errado, **é importante manter uma frequência de revisão e atualização do planejamento**, aplicando ajustes e, principalmente, testes.

Quanto mais completas e realistas forem as simulações, mais segurança poderão agregar à estratégia. Inclua recuperações de aplicações, prática de protocolos de comunicação, ação contra invasões ao sistema, entre outras situações. Quanto mais próxima de um problema real a simulação estiver, **mais preparado o time de TI estará.**

4. Foque na comunicação

A comunicação é um elemento muito importante em uma gestão de crise. Sem ela, nem a equipe com o melhor plano de gestão de crise saberá como agir em algum momento. Como dissemos, é primordial a **figura do porta-voz**, seja da organização como um todo, seja dentro do time de TI. Essa deve ser uma figura que assuma uma postura firme e que não se desespere mesmo quando o cenário for o pior possível. Quando a equipe tiver um bom direcionamento e, somada a isso, uma boa comunicação, será possível **tomar as medidas necessárias sem permitir que o pânico ocupe espaço durante a emergência.**

Assim, mais do que disponibilizar as ferramentas que facilitam a comunicação entre equipes, como os dispositivos móveis e canais de troca de mensagens internas, é aconselhável que a gestão adote uma postura mais aberta ao ouvir as pessoas que trabalham na organização, entendendo suas dúvidas, aceitando as críticas e criando um ambiente de trabalho mais colaborativo.

Viabilize a criação de um protocolo de comunicação de crise, que estabeleça diretrizes para situações de urgência, como alertas de mensagem padrão e comunicados oficiais, por exemplo.

5. Preze pelos seus colaboradores

Treine seus colaboradores para situações de urgência. Isso não significa limitar os treinamentos a simulações de TI, mas desenvolver em cada profissional a perspicácia necessária para sair de situações que possam comprometer sua saúde.

Durante uma crise, por exemplo, é comum que a ansiedade e a incerteza sejam grandes inimigos da produtividade e do bem-estar. **Certifique-se de manter uma relação de confiança e transparência**, para que mesmo em situações difíceis haja motivação e parceria envolvidas na gestão de crise.

6. Assegure o trabalho contínuo

Mesmo diante de uma crise, é certo que uma empresa não pode parar. Muito mais do que a produtividade e o lucro, a empresa está trabalhando para alguém, sejam outras empresas, seja o consumidor final. E é importante considerar essas pessoas — os clientes — durante uma gestão de crise. Em outras palavras, uma organização devidamente preparada para qualquer problema sabe **como manter suas operações mesmo em situações desfavoráveis.**

Para o setor de TI, o **acesso remoto** sem dúvidas é a solução mais significativa para muitos casos. Manter os profissionais com acesso às tecnologias da empresa ainda que não estejam presentes em sua estrutura física é uma forma de manter tudo em andamento, ainda que cada colaborador esteja em um local diferente.

O modelo de trabalho a distância está cada vez mais popular, principalmente pelo incentivo fornecido pela regulamentação do home office no Brasil com a Reforma Trabalhista de 2017. Assim, adotar aos poucos esse modelo evita uma transição brusca em momentos de necessidade, sendo um exemplo de estratégia para empresas que pensam muito à frente dos problemas.

Da mesma forma, **é um erro concentrar todos os dados importantes em um único lugar**. Se uma empresa tiver seu data center comprometido, de nada adiantará ter acesso a ele de qualquer lugar. Invista em data centers adicionais e certifique-se de que a ação de troca possa ser rápida, evitando que as operações sejam interrompidas por muito tempo.

7. Invista em infraestrutura

Preze por uma estrutura segura e confortável para seus colaboradores, tanto nas dependências da empresa quanto em dependências externas. Ou seja, se proponha a assegurar detalhes como alarmes, sensores de incêndio e proteção contra umidade dentro do escritório, assim como a garantir que, para o caso de trabalho remoto, **todos os profissionais disponham do equipamento básico para manter as atividades em execução.**

Conclusão

Podemos ver que a criação de um plano de gestão de crise é muito mais do que criar e colocar no papel um protocolo de ação em cenários negativos. É um processo amplo, que inclui conhecer bem os seus colaboradores, estabelecer a confiança e transparência entre pessoas e processos e, só então, criar estratégias para reduzir ou evitar perdas. Por conseguinte, é impossível fazer tudo isso de uma hora para outra. **É preciso começar o quanto antes**, pois cada momento perdido é uma vulnerabilidade maior em caso de falhas e imprevistos. Se você quer ter um time de TI preparado, com a garantia de que as operações deste setor não serão prejudicadas em tempos de crise, conheça a **NetSupport** e saiba como podemos te ajudar.

NetSupport