



GUIA PRÁTICO

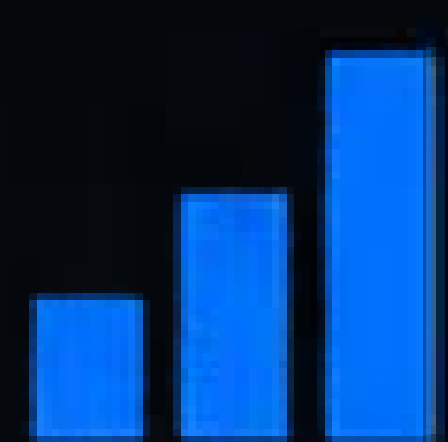
Guia de Análise de Riscos da Infraestrutura

Um material prático para ajudar você a organizar as informações, identificar pontos de atenção e entender os riscos da sua operação.



PREVENÇÃO

Identifique riscos antes que se tornem problemas.



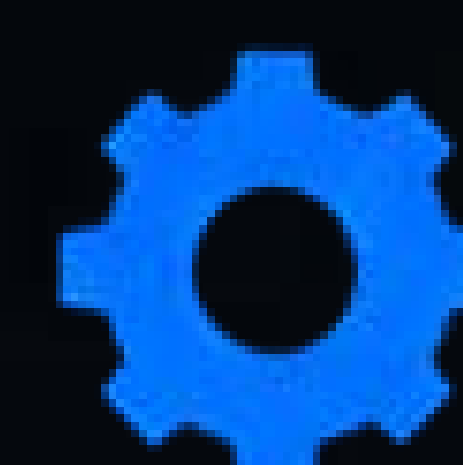
DISPONIBILIDADE

Tenha clareza sobre o que mantém sua operação em funcionamento.



CONTINUIDADE

Planeje ações e reduza o impacto de interrupções.



CONFIABILIDADE

Tome decisões mais seguras com base em informações reais.

Como usar **este guia**

Este material foi criado para ajudar você a organizar informações, identificar pontos de atenção e entender melhor os riscos da sua infraestrutura.

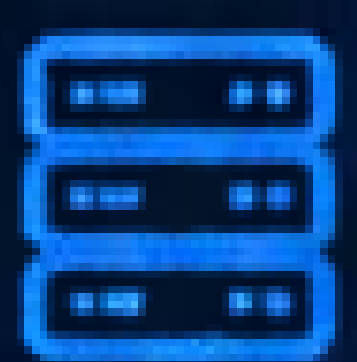
Qual é o **objetivo?**

Fornecer um roteiro prático para que gestores de TI, responsáveis pela infraestrutura e demais líderes possam avaliar, de forma estruturada, os principais riscos de uma interrupção e se preparar melhor para manter a operação em funcionamento.

O que você **vai encontrar?**

O guia está dividido em quatro etapas, que seguem uma lógica simples e objetiva:

01



O que não pode parar?

Identifique os sistemas, processos e equipamentos que são críticos para a sua operação.

02



Quais seriam os impactos de uma interrupção?

Avalie as consequências operacionais, financeiras, de segurança e de imagem.

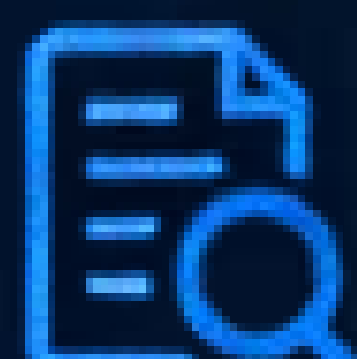
03



Quanto tempo temos para reagir?

Verifique a autonomia, a capacidade de resposta e os procedimentos de contingência.

04



O que ainda precisa ser verificado?

Registre lacunas, defina responsáveis e planeje as próximas ações.



Ao final, **você terá:**



Uma visão mais clara sobre os pontos críticos da sua infraestrutura.



Informações organizadas para priorizar ações.



Maior segurança nas discussões sobre investimentos e melhorias.



Um ponto de partida para conversas mais produtivas com a equipe técnica e fornecedores.



Importante

Este guia é uma ferramenta de orientação para o gestor. Ele ajuda a organizar informações, identificar pontos de atenção e direcionar as próximas ações, mas não substitui uma avaliação técnica da infraestrutura. Para uma análise completa e recomendações personalizadas, conte com o apoio de especialistas da Qidigital.

1. O que não pode parar?

O primeiro passo é identificar quais sistemas, processos e equipamentos são críticos para a operação da sua empresa.



Dica: Para ajudar a definir o que é “crítico” pense em tudo o que, se parar, pode causar prejuízos operacionais, financeiros, de segurança ou de imagem para a sua empresa.

1.1

Sistemas e processos críticos

Liste os principais sistemas, processos e equipamentos que não podem parar.

Item	É crítico?	
	☐ Sim	☐ Não
	☐ Sim	☐ Não
	☐ Sim	☐ Não
	☐ Sim	☐ Não
	☐ Sim	☐ Não

1.2

Priorize os itens

Após listar, classifique a criticidade de cada item (alta, média ou baixa).



Alta

Impacto severo na operação, receita, segurança ou imagem.



Média

Impacto moderado, com possibilidade de contorno ou recuperação.



Baixa

Impacto limitado e de rápida reversão.

1.3

Observações

Registre informações adicionais que consideram relevantes para esta análise.

Ex.: Dependências entre sistemas, observações sobre processos, etc.



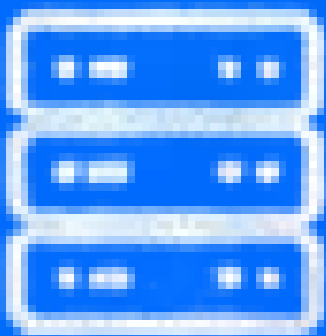
Importante

Esta etapa é fundamental para direcionar as próximas ações. Tenha em mente que a criticidade pode variar conforme o cenário da sua empresa e o contexto do seu negócio.

Identificando o que não pode parar

O primeiro passo é mapear os sistemas, processos e equipamentos que são essenciais para a continuidade da sua operação. Essa identificação ajuda a priorizar o que precisa de maior atenção na análise de riscos.

01

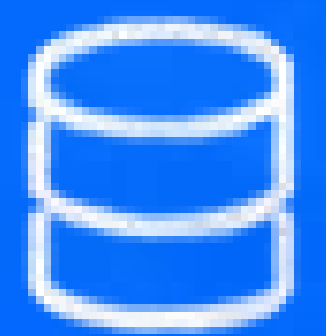


Quais são os sistemas críticos?

Liste os sistemas, aplicações e serviços que não podem parar e justifique por que são essenciais para a operação.

SISTEMA / SERVIÇO	POR QUE É CRÍTICO?	RESPONSÁVEL	OBSERVAÇÕES

02

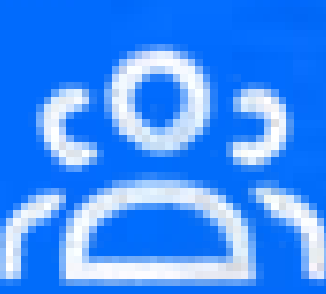


Quais são os equipamentos essenciais?

Identifique os principais equipamentos que sustentam a operação em casos de árvores críticas.

EQUIPAMENTO	FUNÇÃO	LOCALIZAÇÃO	CRÍTICO? (SIM / NÃO)	OBSERVAÇÕES

03



Quais processos dependem deles?

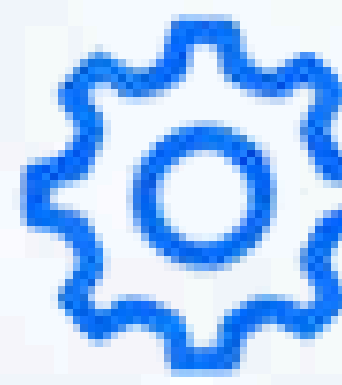
Relateione os principais processos de negócio que seriam afetados em caso de indisponibilidade.

PROCESSO	SISTEMAS / EQUIPAMENTOS RELACIONADOS	CONSEQUÊNCIA PRINCIPAL



Exemplos de sistemas críticos

- ☐ Sistema de gestão (ERP)
- ☐ Servidores de arquivos
- ☐ E-mails corporativos
- ☐ Sistemas de produção
- ☐ Sistemas de segurança (CFTV, controle de acesso)
- ☐ Banco de dados
- ☐ Aplicações em nuvem
- ☐ Internet e rede corporativa
- ☐ Outros: _____



Exemplos de equipamentos essenciais

- ☐ Nobreaks (UPS)
- ☐ Geradores
- ☐ Servidores físicos e virtuais
- ☐ Storages
- ☐ Switches e roteadores
- ☐ Aplicações em nuvem
- ☐ Internet corporativa
- ☐ Quadros elétricos
- ☐ Outros: _____



LEMBRE-SE

Nem tudo tem o mesmo nível de criticidade.

Concentre seus esforços naquilo que realmente impacta a operação da empresa, na segurança das informações e na continuidade do negócio.

Analizando os impactos de uma interrupção

Agora que você já identificou o que não pode parar, é importante avaliar o que pode acontecer em caso de uma interrupção. Isso ajuda a dimensionar os riscos e a priorizar as ações.

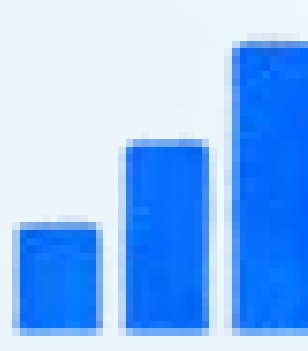
01



Quais seriam as consequências?

Avalie os principais impactos que uma interrupção pode causar para a sua operação.

ÁREA IMPACTADA	DESCRIÇÃO DO IMPACTO	GRAVIDADE (Alta / Média / Baixa)	OBSERVAÇÕES

-  Exemplos de consequências
- ☐ Paralisação da produção
 - ☐ Indisponibilidade de sistemas de atendimento
 - ☐ Perda de dados
 - ☐ Perda de dados
 - ☐ Impacto no faturamento
 - ☐ Multas e penalidades contratuais
 - ☐ Danos à imagem da empresa
 - ☐ Interrupção de serviços essenciais

02



Quais são os impactos financeiros?

Estime os custos envolvidos em uma interrupção, considerando o tempo de indisponibilidade e os processos afetados.

TIPO DE CUSTO	DESCRIÇÃO	ESTIMATIVA (R\$)	OBSERVAÇÕES

-  Exemplos de custos financeiros
- ☐ Perda de receita
 - ☐ Horas extras da equipe
 - ☐ Contratação de serviços emergenciais
 - ☐ Reposição de equipamentos
 - ☐ Outros: _____

03



Quais são os impactos na segurança?

Identifique riscos relacionados à segurança da informação, dados e ambiente físico.

TIPO DE RISCO	DESCRIÇÃO	PROBABILIDADE (Alta / Média / Baixa)	OBSERVAÇÕES

-  Exemplos de riscos de segurança
- ☐ Perda ou corrupção de dados
 - ☐ Exposição de informações sensíveis
 - ☐ Falhas em sistemas de segurança (CFTV, controle de acesso, etc.)
 - ☐ Acesso não autorizado
 - ☐ Comprometimento de backups
 - ☐ Outros: _____



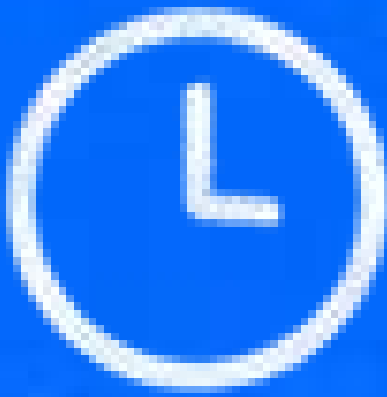
LEMBRE-SE
Nem todos os impactos são imediatos.

Alguns efeitos podem aparecer horas ou dias após a interrupção, como perda de dados, danos à reputação ou impactos em contratos.

Avaliando o tempo de resposta

Saber quanto tempo você tem para reagir é essencial para minimizar os impactos de uma interrupção. Nesta etapa, o objetivo é verificar a autonomia, a capacidade de resposta e os procedimentos de contingência da sua infraestrutura.

01

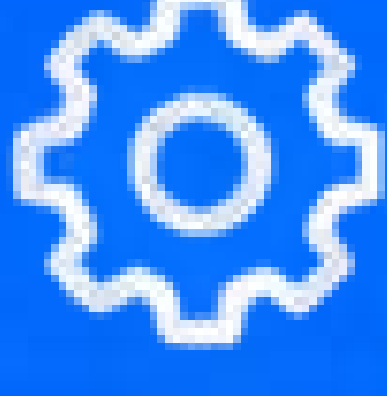


Qual é a autonomia atual?

Verifique por quanto tempo os equipamentos críticos conseguem funcionar em caso de queda de energia.

EQUIPAMENTO / SISTEMA	AUTONOMIA ESTIMADA (EM MINUTOS)	É SUFICIENTE? (SIM / NÃO)	OBSERVAÇÕES

02

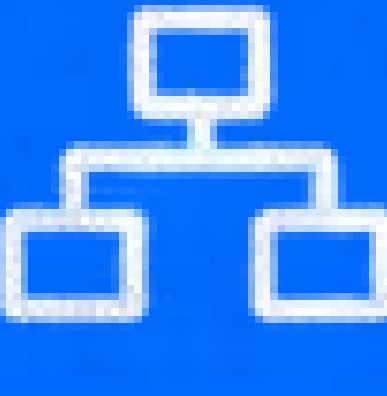


Como é a capacidade de resposta?

Avalie se a equipe, os processos e os recursos são suficientes para uma resposta rápida e eficiente.

ITEM	SITUAÇÃO ATUAL (Adequada / Parcial / Inadequada)	OBSERVAÇÕES
Equipe técnica disponível		
Procedimentos documentados		
Infraestrutura de contingência		
Comunicação com áreas envolvidas		
Suporte de fornecedores		

03



Quais são os procedimentos de contingência?

Registre as ações previstas para manter a operação em caso de interrupção e verifique se estão atualizadas.

CENÁRIO	PROCEDIMENTO ATUAL	RESPONSÁVEL	ÚLTIMA REVISÃO
Queda de energia (curta duração)			
Queda de energia (longa duração)			
Falha em redes			
Falha em redes			
Indisponibilidade de rede			
Outros			



Perguntas para orientar a análise

☐

O tempo de autonomia dos nobreaks é suficiente para os sistemas críticos?

☐

A equipe sabe como agir em caso de interrupção?

☐

Os procedimentos de contingência estão documentados e atualizados?

☐

Há redundância para os equipamentos mais críticos?

☐

Os fornecedores de suporte estão definidos e acessíveis?

☐

Os testes de contingência são realizados periodicamente?



Boas práticas

☐

Realize testes periódicos de autonomia dos nobreaks.

☐

Mantenha os procedimentos de contingência atualizados.

☐

Garanta que a equipe técnica conheça e saiba executar os procedimentos.

☐

Defina contratos de manutenção com a QI

☐

Avalie a necessidade de redundância para sistemas críticos.



Importante

O tempo de resposta pode fazer toda a diferença na continuidade da operação. Uma boa preparação reduz riscos, minimiza prejuízos e garante mais segurança para o negócio.

Verificando o ambiente físico e a energia

O ambiente físico e a infraestrutura de energia são fundamentais para a continuidade da operação. Nesta etapa, avalie as condições das instalações e identifique possíveis riscos que possam afetar a disponibilidade dos sistemas.

01



Como está a infraestrutura elétrica?

Avalie as condições da rede elétrica e dos dispositivos de proteção que garantem o funcionamento de energia.

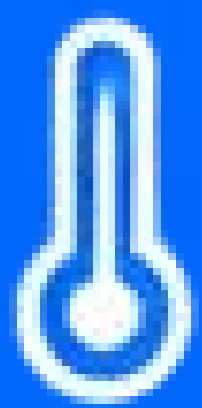
ITEM	SITUAÇÃO ATUAL (Adequada / Parcial / Inadequada)	OBSERVAÇÕES
Rede elétrica estabelecida		
Existência de nobreaks (UPS)		
Capacidade dos nobreaks		
Geradores de energia		
Quadros elétricos em bom estado		
Proteção contra surtos		
Manutenção em dia		



Perguntas para orientar a análise

- ☐ A rede elétrica é estável na sua região?
- ☐ Os nobreaks têm capacidade para suportar os sistemas críticos?
- ☐ As baterias dos nobreaks estão em bom estado e dentro da vida útil?
- ☐ Existe gerador de energia? Ele é testado periodicamente?
- ☐ Os quadros elétricos estão organizados e identificados?
- ☐ Há proteção contra surtos e descargas atmosféricas?
- ☐ A manutenção preventiva está em dia?

02



Como está o ambiente físico?

Verifique as condições do local onde os equipamentos de TI e energia estão instalados.

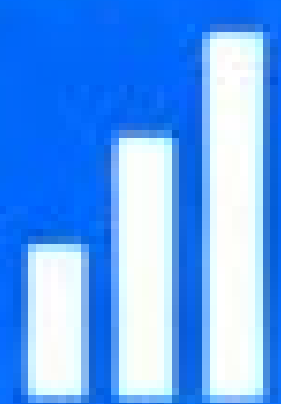
ITEM	SITUAÇÃO ATUAL (Adequada / Parcial / Inadequada)	OBSERVAÇÕES
Controle de temperatura (ar-condicionado)		
Ventilação adequada		
Controle de umidade		
Limpeza e organização		
Segurança física (acesso restrito)		
Proteção contra incêndio		
Espaço físico adequado		



Boas práticas

- ☐ Mantenha a temperatura e a umidade dentro dos limites recomendados.
- ☐ Garanta ventilação e climatização adequadas.
- ☐ Mantenha o ambiente limpo, organize e livre de obstruções.
- ☐ Restrinja o acesso a pessoas autorizadas.
- ☐ Utilize sistemas de detecção e combate à incêndio.
- ☐ Realize inspeções periódicas da infraestrutura física.

03



Há monitoramento e alarmes?

Identifique se há monitoramento contínuo das condições de energia e ambiente.

ITEM	UTILIZAT (SIM / NÃO)	FERRAMENTA / SISTEMA	OBSERVAÇÕES
Monitoramento de energia (nobreaks/geradores)			
Monitoramento de temperatura			
Alarmes em caso de falha			
Notificações para equipe técnica			



Exemplos de ferramentas e soluções

- ☐ Software de monitoramento de nobreaks
- ☐ Monitoramento de temperatura e umidade
- ☐ Sistemas de alarme e notificação (mail, SMS, panel).
- ☐ Monitoramento remoto (ou equipe interna)
- ☐ Interação com sistemas de gestão de infraestrutura



INFRAESTRUTURA SEGURA

Um ambiente bem estruturado reduz riscos, protege seus equipamentos e garante a continuidade da operação.



Qidigital

Consolidando a análise e definindo as próximas ações

Nesta etapa, reúna as informações levantadas, identifique as principais lacunas e defina um plano de ação para reduzir os riscos e aumentar a resiliência da sua operação.

01



Quais são as principais lacunas?

Com base nas análises anteriores, registre o que ainda precisa ser verificado, melhorado ou implementado.

ÁREA	LACUNA IDENTIFICADA	RISCO ASSOCIADO	PRIORIDADE (Alta / Média / Baixa)	RESPONSÁVEL
Sistemas e processos				
Equipamentos				
Tempo de resposta				
Infraestrutura elétrica				
Ambiente físico				
Segurança da informação				
Monitoramento				
Outros				

02

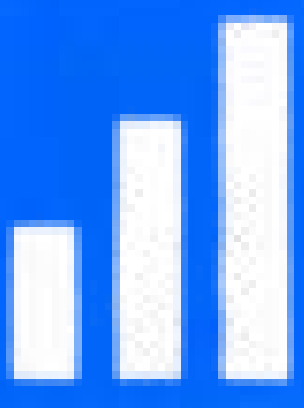


Qual é o plano de ação?

Defina as próximas ações, as responsáveis e os prazos para tratar as lacunas identificadas.

AÇÃO	RESPONSÁVEL	PRAZO	STATUS (Não Iniciado / Em andamento / Concluído)

03



Acompanhamento e revisão

A análise de riscos deve ser revisada periodicamente ou sempre que houver mudanças na infraestrutura, nos sistemas ou no negócio.

DATA DA REVISÃO	PRINCIPAIS ATUALIZAÇÕES	RESPONSÁVEL	OBSERVAÇÕES



Exemplos de ações para reduzir os riscos

- ☐ Atualizar ou substituir equipamentos obsoletos
- ☐ Implementar redundância em sistemas críticos
- ☐ Revisar e testar procedimentos de contingência
- ☐ Realizar manutenções preventivas periódicas
- ☐ Implementar monitoramento contínuo
- ☐ Treinar equipe para atuação em caso de falhas
- ☐ Revisar contratos de suporte e manutenção
- ☐ Revisar as condições do ambiente físico e de energia
- ☐ Outros: _____



Checklist final

Antes de finalizar a sua análise, confirme os principais pontos:

- ☐ Identifique os sistemas e processos críticos
- ☐ Avalie os impactos de uma interrupção
- ☐ Verifique o tempo de resposta e autonomia
- ☐ Analise os equipamentos e a infraestrutura
- ☐ Registre as principais lacunas
- ☐ Defina as próximas ações



LEMBRE-SE

Este guia é um ponto de partida.

Ele ajuda os gestores a organizar as informações, identificar pontos de atenção e direcionar as próximas ações. Para uma análise completa e personalizada, conte com o apoio de especialistas.



Qidigital

FALE COM UM ESPECIALISTA

Mais segurança e continuidade para o seu negócio.