

[linha decorativa]

**Commented [AES1]:** Para aprender como preencher este documento, e ver exemplos reais do que você precisa escrever, veja este vídeo tutorial "How to Write Business Continuity Strategy According to ISO 22301".  
  
Para acessar o tutorial: Em sua caixa de entrada, encontre o e-mail que você recebeu no momento da compra. Lá, você verá um link e uma senha que lhe permitirá acessar o vídeo tutorial.

[logotipo da organização]  
[nome da organização]

**Commented [AES2]:** Todos os campos desse documento que aparecem entre colchetes devem ser preenchidos.

## ESTRATÉGIA DE CONTINUIDADE DE NEGÓCIOS

**Commented [AES3]:** Aprenda mais sobre estratégia de continuidade de negócios aqui:  
  
A estratégia de continuidade de negócios pode ajudá-lo a economizar dinheiro? <https://advisera.com/27001academy/pt-br/blog/2010/12/16/a-estrategia-de-continuidade-de-negocios-pode-ajuda-lo-a-economizar-dinheiro/>

Código:	
Versão:	
Data da versão:	
Criado por:	
Aprovado por:	
Nível de confidencialidade:	

**Commented [AES4]:** O sistema de codificação do documento deve estar de acordo com o atual sistema de codificação de documentos da organização. Caso não haja um sistema desse tipo na organização, esta linha pode ser excluída.

## Histórico de alterações

Data	Versão	Criado por	Descrição da alteração
	0.1	Advisera	Esboço básico do documento

## Sumário

<b>1. FINALIDADE, ESCOPO E USUÁRIOS .....</b>	<b>4</b>
<b>2. DOCUMENTOS DE REFERÊNCIA .....</b>	<b>4</b>
<b>3. SOBRE A ESTRATÉGIA.....</b>	<b>4</b>
3.1. ANÁLISE DE IMPACTO NOS NEGÓCIOS.....	4
3.2. GESTÃO DE RISCOS.....	4
<b>4. ESTRUTURA DE RESPOSTA A INCIDENTES.....</b>	<b>5</b>
4.1. EQUIPE DE GESTÃO DE CRISES E EQUIPE DE SUPORTE À GESTÃO DE CRISES .....	5
4.1.1. <i>Equipe de gestão de crises</i> .....	5
4.1.2. <i>Equipe de suporte à gestão de crises</i> .....	5
4.1.3. <i>Equipamentos da Central de comando</i> .....	6
4.2. GERAÇÃO DE RELATÓRIOS E TOMADA DE DECISÕES .....	7
4.3. COOPERAÇÃO COM AUTORIDADES.....	8
4.4. EVACUAÇÃO E DE PRÉDIO E PONTOS DE MONTAGEM .....	9
4.5. MEIOS DE COMUNICAÇÃO .....	9
4.6. TRANSPORTE PARA LOCAIS ALTERNATIVOS .....	9
4.7. COMUNICAÇÃO COM AS PARTES INTERESSADAS .....	10
<b>5. ESTRATÉGIA DE RECURSOS.....</b>	<b>10</b>
5.1. LOCAIS E SOLUÇÕES DE INFRAESTRUTURA .....	10
5.2. SOLUÇÕES DE FORNECEDORES E PARCEIROS DE TERCEIRIZAÇÃO .....	12
5.3. SOLUÇÕES DE APLICATIVOS/BANCOS DE DADOS .....	13
5.4. SOLUÇÕES DE DADOS.....	13
5.5. CONTENÇÃO DE UM PONTO ÚNICO DE FALHA.....	14
5.6. PROVEDO RECURSOS FINANCEIROS .....	14
<b>6. ESTRATÉGIA DE RECUPERAÇÃO PARA ATIVIDADES INDIVIDUAIS.....</b>	<b>15</b>
<b>7. IMPLEMENTAÇÃO DE TODOS OS PREPARATIVOS NECESSÁRIOS.....</b>	<b>15</b>

---

8. GESTÃO DE REGISTROS MANTIDOS DE ACORDO COM ESTE DOCUMENTO.....	15
9. VALIDADE E GESTÃO DE DOCUMENTOS.....	16
10. ANEXOS .....	16

### 1. Finalidade, escopo e usuários

A finalidade deste documento é definir quais opções e soluções a [nome da organização] garantirá que todas as condições para a retomada das atividades comerciais em caso de desastres ou outro incidente disruptivo sejam atendidas. Ela é a base para a elaboração do Plano de continuidade de negócios e de planos de recuperação.

**Commented [AES5]:** Inclua o nome da sua organização.

Este documento aplica-se a todo o escopo do Sistema de Gestão da Continuidade de Negócios (SGCN), conforme definido na Política de continuidade de negócios.

Os usuários deste documento são membros da alta direção e pessoas responsáveis pela implementação do projeto de gestão da continuidade de negócios.

### 2. Documentos de referência

- Norma ISO 22301, cláusulas 8.3 e 8.4.2
- Política de continuidade de negócios
- Questionários de análise de impacto nos negócios
- [Documento de avaliação de riscos]
- [Documento de tratamento de riscos]
- O Plano de continuidade de negócios que contém o Plano de resposta a incidentes e planos de recuperação

**Commented [AES6]:** Você pode encontrar um modelo para este documento na pasta "06\_Avaliacao\_e\_tratamento\_de\_riscos" do Kit de documentação Premium da ISO 27001 e ISO 22301.

**Commented [AES7]:** Você pode encontrar um modelo para este documento na pasta "06\_Avaliacao\_e\_tratamento\_de\_riscos" do Kit de documentação Premium da ISO 27001 e ISO 22301.

### 3. Sobre a estratégia

Esta Estratégia e soluções relacionadas são elaboradas com base nos resultados da análise de

**Commented [AES8]:** Soluções referem-se a respostas organizacionais (por exemplo, políticas e procedimentos), técnicas (por exemplo, equipamentos e métodos) ou pessoais (por exemplo, treinamento) implementadas para cumprir estratégias.

#### 3.1. Análise de impacto nos negócios

A análise de impacto nos negócios determina que [especifique a quantidade] atividades oferecem suporte aos principais produtos e serviços; consulte o Anexo 1 – Objetivos de tempo de recuperação para atividades para obter a lista dessas atividades.

**Commented [AES9]:** Inclua aqui o número de atividades

O Anexo 1 – Objetivos de tempo de recuperação para atividades também determina os objetivos de tempo de recuperação para cada atividade crítica, levando em consideração a dependência de outras atividades.

**Commented [AES10]:** Para saber mais sobre o assunto, leia este artigo:

O Anexo 1 – Objetivos de tempo de recuperação para atividades também determina os objetivos de tempo de recuperação para cada atividade crítica, levando em consideração a dependência de outras atividades.

**Commented [AES11]:** Para entender a diferença entre análise de impacto nos negócios e gestão de riscos, leia este artigo:

#### 3.2. Gestão de riscos

A avaliação dos riscos que podem afetar a continuidade de negócios é descrita em [nome do documento]. Os riscos mais altos que podem resultar em um incidente disruptivo, isto é, a interrupção nos negócios identificada durante a avaliação de riscos, são:

- [lista]

Para todos os riscos/incidentes mencionados é necessário:

- aplicar ações preventivas para reduzir a probabilidade desse incidentes – as ações estão descritas em [nome do documento]
- aplicar ações preventivas para diminuir as possíveis consequências desses incidentes – essas ações também estão descritas em [nome do documento]

O [cargo] é responsável pela elaboração de ações preventivas e o [cargo] é responsável pela

#### 4. Estrutura de resposta a incidentes

##### 4.1. Equipe de gestão de crises e Equipe de suporte à gestão de crises

###### 4.1.1. Equipe de gestão de crises

Se os planos de continuidade de negócios forem ativados, um órgão chamado Equipe de gestão de crises é formado e tem autorização para tomar as decisões necessárias para solucionar a situação. Os membros do Equipe de gestão de crises são:

- [todos os membros da alta direção]
- [pessoa do departamento de relações públicas]
- [pessoa do departamento de recursos humanos]

O Equipe de gestão de crises é gerenciado pelo gerente de crises. O [cargo] desempenhará a função de gerente de crises e no caso de sua ausência, a função será realizada pelo [cargo].

###### 4.1.2. Equipe de suporte à gestão de crises

Commented [AES12]: Inclua aqui o nome do documento de

Commented [AES13]: Liste todos os riscos inaceitáveis ou de

Commented [AES14]: Se a avaliação de riscos foi realizada de

Commented [AES15]: Se a avaliação de riscos foi realizada de

Commented [AES16]: Você pode encontrar um modelo para este documento na pasta

Commented [AES17]: Ex.: gerente de continuidade de

Commented [AES18]: Ex.: gerente de continuidade de

Commented [AES19]: Ações preventivas e Plano de resposta a

Commented [AES20]: Para saber mais sobre estruturas de gestão de incidentes, leia este artigo:

Commented [AES21]: Para saber mais sobre o assunto, leia este artigo:

Commented [AES22]: Adapte-se ao sistema de nomenclatura

Commented [AES23]: Avalie se essas são as melhores funções para o gestão da crises com competência.

Por exemplo, as seguintes capacidades devem estar presentes:  
- pessoa que irá lidar com a comunicação com várias partes interessadas (incluindo a mídia pública)

Commented [AES24]: Geralmente alguém com autoridade e

O [Equipe de suporte à gestão de crises] tem a função de absorver as atividades administrativas e

Commented [AES25]: Adapte-se ao sistema de nomenclatura

Os membros do Equipe de suporte à gestão de crises são:

- [secretários]
- [messageiros]

Commented [AES26]: Estes são apenas exemplos.

O Equipe de suporte à gestão de crises deverá trabalhar nos locais especificados pelo Equipe de gestão de crises.

4.1.3. Equipamentos da Central de comando

Para atender ao Equipe de suporte à gestão de crises e ao Equipe de gestão de crises, a Central de comando deve estar equipada da seguinte forma:

Nome do recurso	Descrição	Quantidade	Quando o recurso é necessário
<b>Aplicativos/bancos de dados:</b>			
<b>Dados armazenados em formato eletrônico:</b>			
<b>Dados armazenados em papel:</b>			

Commented [AES27]: Dependendo da quantidade de

<b>Equipamentos de TI e comunicações:</b>			
<i>Estações de trabalho</i>			<i>[em duas horas]</i>
<i>Telefones</i>			<i>imediatamente</i>
<b>Canais de comunicação:</b>			
<i>Linhas telefônicas fixas</i>			<i>imediatamente</i>
<b>Outros equipamentos:</b>			
<i>Televisão</i>			<i>imediatamente</i>
<b>Instalações e infraestrutura:</b>			
<i>Rede de computadores</i>			<i>[em duas horas]</i>
<b>Serviços externos:</b>			

O [cargo] é responsável por preparar os membros do Equipe de gestão de crises e do Equipe de

**Commented [AES28]:** Ex.: gerente de continuidade de  
**Commented [AES29]:** Geralmente é alguém com antiguidade

#### 4.2. Geração de relatórios e tomada de decisões

Os incidentes são relatados da seguinte forma:

- todos os incidentes relacionados à tecnologia de TI e comunicações são informados a [cargo] ou nome da unidade organizacional

**Commented [AES30]:** Este é um exemplo do processo de tomada de decisões em duas etapas relacionado a incidentes, que  
**Commented [AES31]:** Ex.: chefe do departamento de TI  
**Commented [AES32]:** Ex.: oficial de segurança

Se as pessoas mencionadas não puderem solucionar o incidente, o gerente de crises deve ser

As autorizações para a tomada de decisões são:

<i>Tipo de decisão</i>	<i>Quem está autorizado</i>
Como pequenos incidentes relacionados à tecnologia de TI e comunicações são solucionados	Funcionários da [nome da unidade organizacional]
Como todos os demais pequenos incidentes são solucionados	Funcionários da [nome da unidade organizacional]
Seleção de informações a serem fornecidas à mídia durante um incidente disruptivo	[cargo]

**Commented [AES33]:** Geralmente é alguém com antiguidade

**Commented [AES34]:** Ex.: gerente de compras

**Commented [AES35]:** Ex.: analista de compras

O [cargo] é responsável por preparar os funcionários da [nome da unidade organizacional] para

**Commented [AES36]:** Ex.: chefe do departamento de TI

**Commented [AES37]:** Ex.: gerente de continuidade de negócios

### 4.3. Cooperação com autoridades

As seguintes pessoas são responsável pela coordenação com autoridades estatais e serviços de emergência:

<i>Autoridade</i>	<i>Quem é responsável</i>
Polícia	[cargo]

**Commented [AES38]:** Liste outras autoridades relevantes para

As pessoas mencionadas devem implementar todas as atividades preliminares para garantir que a interoperabilidade com as autoridades durante um incidente disruptivo seja satisfatória.



Informações necessárias em caso de um incidente disruptivo e como a organização se recuperará.

#### 4.4. Evacuação e de prédio e pontos de montagem

Todos os prédios são evacuados conforme especificado no plano de evacuação de prédios em caso de incêndio.

Após a evacuação, os funcionários devem reunir-se nos seguintes pontos de montagem:

	Ponto de montagem 1	Ponto de montagem 2
[endereço do local nº. 1]		
[endereço do local nº. 2]		
[endereço do local nº. 3]		
[endereço do local nº. 4]		

Nota: se o Ponto de montagem 1 não estiver disponível, os funcionários devem dirigir-se ao Ponto de montagem 2.

Informações necessárias em caso de um incidente disruptivo e como a organização se recuperará.

#### 4.5. Meios de comunicação

Os seguintes soluções de comunicação serão usados em caso de um incidente disruptivo (os meios que aparecem no topo da lista devem ser usados primeiros; os que aparecem na parte inferior da lista só devem ser usados em caso de indisponibilidade do restante dos meios):

1. telefones móveis (corporativos e pessoais)
2. telefones (corporativos e pessoais)
3. [redacted]
4. [redacted]
5. mensageiros (funcionários da organização ou serviços especializados)
6. [estações portáteis – indique onde elas estão armazenadas e que tem direito de usá-las]
7. [redacted]
8. [redacted]

O [cargo] é responsável pela aquisição/preparação e, quando necessário, pela manutenção dos

meios de comunicação necessários para garantir que todos os funcionários tenham um método de comunicação.

#### 4.6. Transporte para locais alternativos

Os funcionários da organização serão transportados do local principal para o local alternativo das seguintes formas:

**Commented [AES39]:** Se este tipo de plano não existir, é necessário ter um plano de evacuação.

**Commented [AES40]:** Estes locais geralmente são externos (portanto, não são ameaçados em caso de terremoto), distantes o suficiente para não serem afetados por um terremoto.

**Commented [AES41]:** Ex.: gerente de continuidade de negócios.

**Commented [AES42]:** Para saber mais sobre o assunto, leia este artigo: [link]

**Commented [AES43]:** Estes são apenas exemplos. Você pode excluir ou adicionar novas formas de comunicação com base nas práticas da sua organização.

**Commented [AES44]:** Ex.: gerente de continuidade de negócios.

Atividade	Meios de transporte
Equipe de gestão de crises e Equipe de suporte à gestão de crises	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]

**Commented [AES45]:** Uma forma de transporte adequada

**Commented [AES46]:** Liste todas as atividades.

O [cargo] é responsável por fornecer todos os meios de transporte.

**Commented [AES47]:** Ex.: gerente de instalações

#### 4.7. Comunicação com as partes interessadas

A [nome da organização] designará pessoas para comunicar-se com as partes interessadas em caso de um incidente disruptivo seguindo os métodos de comunicação a seguir:

**Commented [AES48]:** Inclua o nome da sua organização.

	[Telefone]	[Reuniões]	[E-mail]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Funcionários]							
[Proprietários/partes interessadas]							
[Famíliares de funcionários]							
[Redacted]							
[Redacted]							
[Redacted]							
[Redacted]							

**Commented [AES49]:** Para cada meio de comunicação

O [cargo] é responsável por preparar todas as pessoas mencionadas acima para comunicação durante o incidente disruptivo.

**Commented [AES50]:** Ex.: gerente de continuidade de negócios

[Redacted]

**Commented [AES51]:** Ex.: gerente de continuidade de

### 5. Estratégia de recursos

#### 5.1. Locais e soluções de infraestrutura

Os locais de recuperação da [nome da organização] são:

Nome	Local principal	Estratégia para local alternativo	Quantidade mínima de locais de trabalho	Soluções de equipamentos *	Local alternativo – próximo	Local alternativo – distante
Central de comando	[endereço]	[a] locais alternativos na organização (por exemplo, se a organização possui outros locais à sua disposição);  d) locais alternativos fornecidos por organizações especializadas (por exemplo, organizações que alugam suas instalações em caso de desastres, mas também hotéis ou instituições de		[a] frio, b) morno,	[endereço]	[endereço]

**Commented [AESS3]:** Este local geralmente está localizado na

**Commented [AESS4]:** Este local geralmente está localizado a pelo menos 40 km do local principal.

**Commented [AESS2]:** Dependendo da quantidade de pessoas

		ensino equipadas com infraestrutura de informação e comunicação);				
[nome da atividade]	[endereço]				[endereço]	[endereço]

Commented [AES55]: Seleccione para cada atividade crítica e

Commented [AES56]: Liste todas as atividades, incluindo o

\*Os termos usados nesta coluna têm o seguinte significado:

- a) frio – um local sem infraestrutura ou equipamentos
- b) morno – um local com infraestrutura básica (rede, entre outros elementos), links e equipamentos cujo tempo de compra são longos pré-instalados

O [cargo] é responsável por todos os ajustes necessários em relação aos locais alternativos.

Commented [AES57]: Ex.: gerente de instalações

### 5.2. Soluções de fornecedores e parceiros de terceirização

As relações com os fornecedores e parceiros de terceirização devem ser gerenciadas da seguinte forma:

Nome do fornecedor/parceiro de terceirização	Estratégia
	[a] os serviços são contratados de diversos fornecedores e parceiros de terceirização simultaneamente – se um parceiro estiver indisponível, é possível usar os serviços de outro parceiro)

Commented [AES58]: Forneça os nomes de todos os

	<p>c) obrigação de fornecedores/parceiros de terceirização, por contrato, a fornecer produtos ou serviços independentemente de incidentes disruptivos e definição de penalidades, dessa forma, os fornecedores/parceiros de terceirização são obrigados a introduzir a continuidade de negócios, e transferência de parte dos riscos financeiros para eles</p>

Commented [AES59]: Selecione uma ou mais das opções

O [cargo] é responsável por gerenciar as relações com os fornecedores e parceiros de terceirização

Commented [AES60]: Ex.: gerente de compras, gerente de instalações

**5.3. Soluções de aplicativos/bancos de dados**

Todos os aplicativos e bancos de dados necessários serão instalados no local alternativo se forem necessários em até 24 horas após o incidente disruptivo; a mídia de instalação dos aplicativos e bancos de dados que não forem necessários nesse período de tempo será armazenada no local alternativo.

Commented [AES61]: Ex.: gerente de TI

**5.4. Soluções de dados**

As cópias de segurança de dados compartilhadas pelas atividades devem ser feitas com a seguinte periodicidade:

Nome do aplicativo, do banco de dados, da pasta, do documento	Frequência da criação de cópias de segurança	Procedimento para cópias de segurança
		[a] aplicativos/bancos de dados - procedimento automatizado de criação de cópias de segurança com base no servidor;

Commented [AES62]: Copie do Questionário de análise de

Commented [AES63]: A frequência é determinada com base

		<small>Resposta alternativa Resposta alternativa Resposta alternativa Resposta alternativa Resposta alternativa Resposta alternativa Resposta alternativa Resposta alternativa Resposta alternativa Resposta alternativa Resposta alternativa Resposta alternativa Resposta alternativa Resposta alternativa Resposta alternativa Resposta alternativa</small>

**Commented [AES64]:** Selecione a estratégia adequada de...

Nota: a frequência de criação das cópias de segurança dos dados usadas por uma única atividade é definida na estratégia da atividade em questão.

[Comentário] responder uma cópia de segurança dos dados armazenada...

**Commented [AES65]:** Se houver diversos grupos de dados, um...

### 5.5. Contenção de um Ponto único de falha

As seguintes estratégias são usadas para evitar um Ponto único de falha que pode causar a interrupção de uma atividade:

<b>Ponto único de falha</b>	<b>Atividade no local ocorrido</b>	<b>Estratégia de contenção</b>

**Commented [AES66]:** Copie do Questionário de análise de...

**Commented [AES67]:** Planeje recursos alternativos ou de...

[Comentário] responder uma implementação de estratégia de contenção de Ponto único de falha...

**Commented [AES68]:** Se houver vários tipos de Pontos únicos...

### 5.6. Provendo recursos financeiros

A [nome da organização] requer [quantidade em moeda local] de capital de giro para todas as atividades, mais [quantidade em moeda local] para compras de emergência caso um incidente disruptivo ocorra.

Em caso de um incidente disruptivo, os recursos financeiros serão fornecidos de acordo com o plano de contingência de emergência. O plano de contingência de emergência deve ser atualizado regularmente para refletir as mudanças no cenário de negócios e no mercado.

O [cargo] é responsável por manter todos os acordos necessários relacionados à provisão de recursos financeiros.

Commented [AES69]: Inclua o nome da sua organização.

Commented [AES70]: Calcule a partir dos Questionários de

Commented [AES71]: Calcule o custo de todos os recursos que

Commented [AES72]: Especifique outros instrumentos

Commented [AES73]: Geralmente é alguém com antiguidade

### 6. Estratégia de recuperação para atividades individuais

A estratégia de recuperação de atividades individuais e soluções para implementar estas estratégias são definidas nos anexos 4 a [número] desta Estratégia.

As soluções de recuperação para atividades individuais e soluções para implementar estas estratégias são definidas nos anexos 4 a [número] desta Estratégia.

Commented [AES74]: Geralmente é alguém com antiguidade

### 7. Implementação de todos os preparativos necessários

O Anexo 3 – Plano de preparação para a continuidade de negócios lista todos os preparativos necessários para a implementação nesta Estratégia e soluções relacionadas.

O Anexo 3 – Plano de preparação para a continuidade de negócios lista todos os preparativos necessários para a implementação nesta Estratégia e soluções relacionadas.

Commented [AES75]: Geralmente é alguém com antiguidade

Commented [AES76]: Ex.: gerente de continuidade de

### 8. Gestão de registros mantidos de acordo com este documento

Nome do registro	Local de armazenamento	Responsável pelo registro	Período de retenção do registro	Período de revisão
Plano de preparação para a continuidade de negócios (em formato eletrônico)	Computador de [cargo responsável por monitorar a execução]	[cargo responsável pelo registro]	[período de retenção do registro]	[período de revisão]

Commented [AES77]: Adapte o período desta coluna às suas

Commented [AES78]: Ex.: gerente de continuidade de

## 9. Validade e gestão de documentos

Este documento é válido a partir de [data].

*Este procedimento de documentos é obrigatório para todos os setores e, se necessário, alterar o documento para refletir a realidade da organização.*

Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios devem ser considerados:

- se a organização foi bem-sucedida na recuperação das atividades no objetivo de tempo de recuperação
- se todos os procedimentos necessários para a continuidade de negócios foram implementados

## 10. Anexos

- Anexo 1 – Objetivos de tempo de recuperação para atividades
- Anexo 2 – Exemplos de cenários de incidentes disruptivos
- Anexo 3 – Plano de continuidade para a continuidade de negócios
- Anexo 4 – Modelo de matriz de continuidade de atividades para setores de atividades

[cargo]

[nome]

[assinatura]

Commented [AES79]: Ex.: gerente de continuidade de

Commented [AES80]: Isso é apenas uma recomendação;

Commented [AES81]: Insira para cada atividade crítica, a

Commented [AES82]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.