POLÍTICA DE

GESTÃO DE RISCO (T.I.)

POLI-0005-01

MANTENHA APENAS UM: CONFIDENCIAL | **RESTRITO** | USO INTERNO | PÚBLICO

Obs. Este documento contou com a contribuição da Innocenti Advogados (consultora externa)

Controle de Versões

Data	Versão	Comentários	Autor
01.06.2021	1.0	Versão Inicial	Mariana M. Carregaro
13.01.2024	2.0	Revisão	Mariana M. Carregaro
13.01.2025	3.0	Revisão	Mariana M. Carregaro

Identificação e Classificação

Código do Documento	Tipo	Classificação
POLI-0005-01	Política	Restrito

Equipe e Responsáveis Envolvidos

Profissionais Envolvidos
Mariana M. Carregaro – Consultora Externa (Innocenti Advogados)
Lidiane P. dos Reis Barros – Encarregada

Documentos de Apoio ou Relacionados

Documentos de Apoio
Política de Segurança da Informação (T.I.)
Política de Incidente de Segurança (T.I.)
Política de Gestão de Continuidade do Negócio (T.I.)
Política de Backup e Restauração (T.I.)
Política de Notificação de Violação (T.I.)
Evidência e Controle das Vulnerabilidades Cibernéticas

Aprovação da Diretoria Responsável

Diretor Responsável	Ratificação	Data
Alexandre Gonçalves Duarte	APROVADO	13.01.2025

Introdução

A ausência de uma Política de Gestão de Riscos pode comprometer o alcance dos objetivos da **Epeople**, colocando em risco a sua finalidade maior: o atendimento ao seu cliente.

Destaca-se que os riscos também podem revelar oportunidades (riscos positivos). Nesse caso, o gestor deve potencializá-los para melhor aproveitá-los.

Conceitos

A Política de Gestão de Riscos é uma demonstração clara e evidente de que a **Epeople** está atenta ao cenário mundial, momento em que as instituições públicas e privadas vêm investindo cada vez mais em controles internos e ações de prevenção a eventos que possam impactar o alcance de seus objetivos.

É uma norma que traz de forma consolidada as principais normas internacionais que tratam da gestão de riscos corporativos, como o COSO ERM e a ISO 31000:2009.

O presente documento traz as linhas gerais e as intenções da alta administração da **Epeople** no gerenciamento de seus riscos institucionais, apresentando a seguinte estrutura:

- ✓ Princípios;
- ✓ Objetivos;
- ✓ Conceitos;
- ✓ Competências dos gestores de riscos;
- ✓ Diretrizes para o gerenciamento de riscos;
- ✓ Processo de gerenciamento de riscos; e
- ✓ Informações requeridas para o gerenciamento de riscos (MAPA DE RISCOS).

Princípios

A Política de Gestão de Riscos da **Epeople** observará os seguintes princípios:

- ✓ **AGREGAR** valor e proteger o ambiente institucional;
- ✓ **SER** parte integrante dos processos organizacionais;
- ✓ **SUBSIDIAR** a tomada de decisões;
- ✓ **ABORDAR** explicitamente a incerteza;
- ✓ **SER** sistemática, estruturada e oportuna;
- ✓ **SER** baseada nas melhores informações disponíveis;
- ✓ **SER** feita sob medida, alinhada com o contexto interno e externo da **Epeople**, e com o perfil do risco;
- ✓ **CONSIDERAR** fatores humanos e culturais;
- ✓ **SER** transparente e conclusiva;
- ✓ **SER** dinâmica, interativa e capaz de reagir a mudanças; e
- ✓ **APOIAR** a melhoria contínua da entidade.

Objetivos

A Política de Gestão de Riscos visará ao **DESENVOLVIMENTO**, **DISSEMINAÇÃO** E **IMPLEMENTAÇÃO** de metodologias de gerenciamento de riscos institucionais, objetivando apoiar a melhoria contínua de processos de trabalho, projetos e a alocação e utilização eficaz dos recursos disponíveis, contribuindo para o cumprimento dos objetivos da **Epeople**.

Gestores de Riscos

São considerados gestores de riscos, assim entendidos aqueles que são os titulares responsáveis pelo gerenciamento dos riscos em seus respectivos âmbitos e escopos de atuação, o **Diretor-Presidente**, os **Diretores**, os **Gerentes-Gerais**, os **Gerentes**, os **Coordenadores** ou equivalentes, responsáveis por processos de trabalho, projetos e iniciativas estratégicas, táticas e operacionais da **Epeople**.

Competência dos Gestores de Riscos

Compete aos gestores de riscos, relativamente aos processos de trabalho e projetos sob sua responsabilidade:

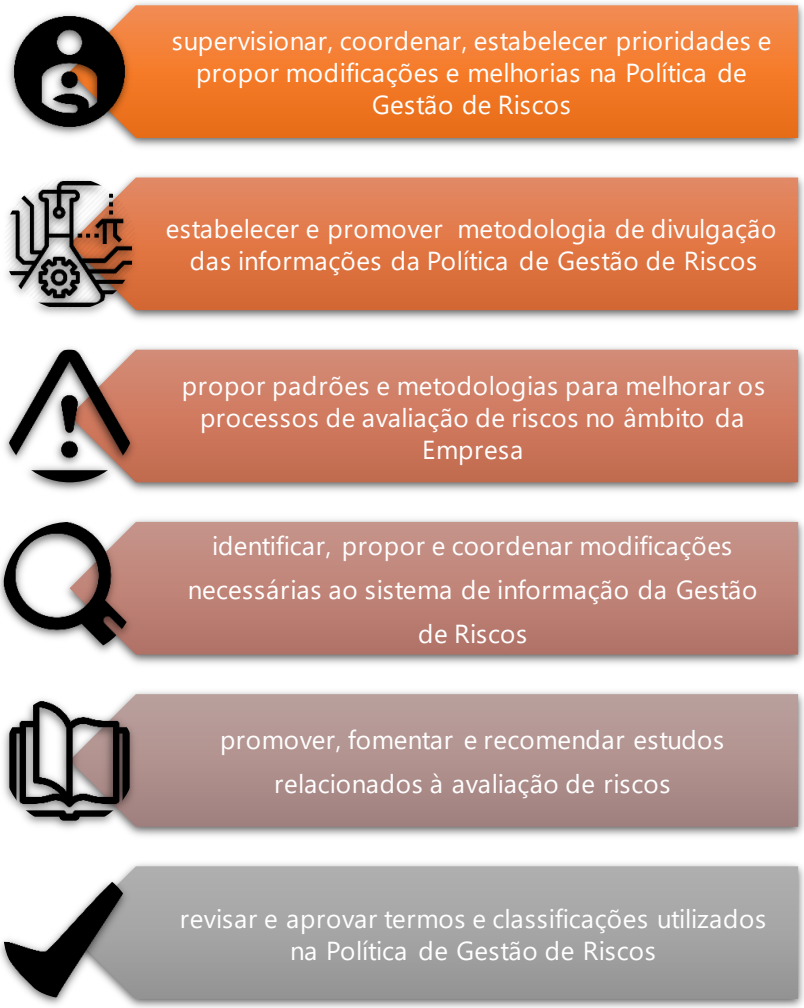
Decidir sobre a escolha dos processos de trabalho que devam ter os riscos gerenciados e tratados com prioridade em cada unidade administrativa, à vista da dimensão dos prejuízos e dos impactos que possam causar, sob os aspectos estratégico, orçamentário, e de imagem

Estabelecer as ações de tratamento ou monitoramento a serem implementados bem como fixar prazo de implementação e avaliar os resultados obtidos

Definir quais riscos deverão ser priorizados para tratamento por meio de ações de caráter imediato, curto prazo, médio prazo ou longo prazo ou de ações de aperfeiçoamento contínuo bem como fixar prazo para implementação e avaliar os resultados obtidos por meio de indicadores.

Comitê de Avaliação de Riscos

O Comitê de Avaliação de Riscos, de caráter consultivo, sob coordenação da Presidência da **Epeople**, tem as seguintes atribuições:



Diretrizes para o Gerenciamento de Riscos

O gerenciamento de riscos deve ser feito em ciclos **NÃO SUPERIORES A DOIS ANOS**, abrangendo os processos de trabalho, sistemas informatizados, gestão orçamentária, gestão de pessoas e legislação, com vistas a reduzir os eventos de riscos negativos, assim como, quando for o caso, potencializar os eventos de riscos positivos (oportunidades).

O limite temporal a ser considerado para o ciclo de gerenciamento de riscos de cada processo de trabalho será decidido pelo respectivo gestor, levando em conta o limite máximo estipulado anteriormente.

Como tratar o Risco

01

EVITAR OS RISCOS:

Não iniciando ou descontinuando a atividade que dá origem ao risco

02

ELIMINAR OS RISCOS:

Removendo a respectiva fonte causadora

03

ACEITAR OS RISCOS:

Assumindo o risco, por uma escolha consciente e justificada formalmente, podendo implementar sistemática de monitoramento

04

REDUZIR OS RISCOS:

Mitigar e reduzir o risco verificado

05

COMPARTILHAR O RISCO

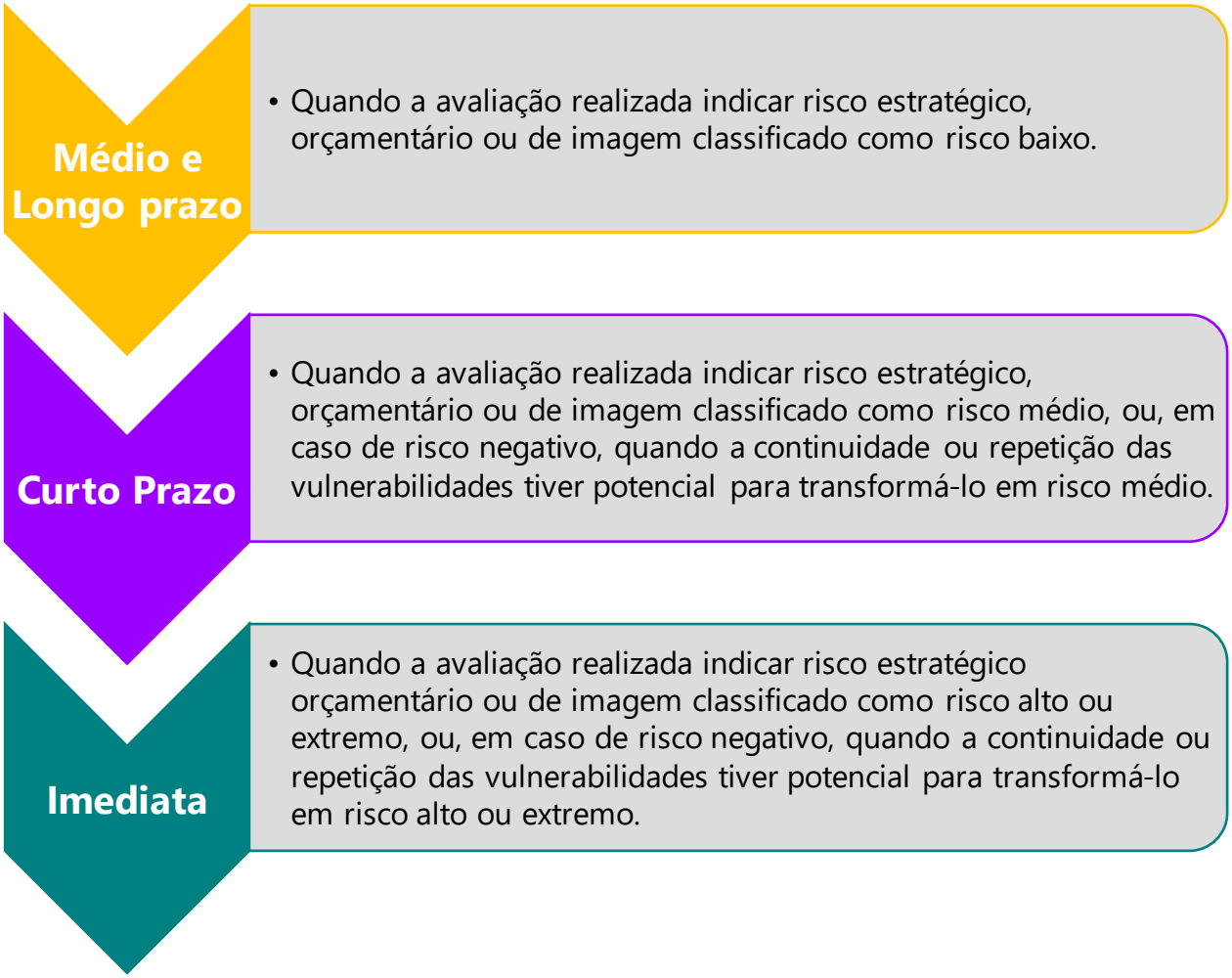
Com outras partes interessadas

06

AUMENTAR O RISCO

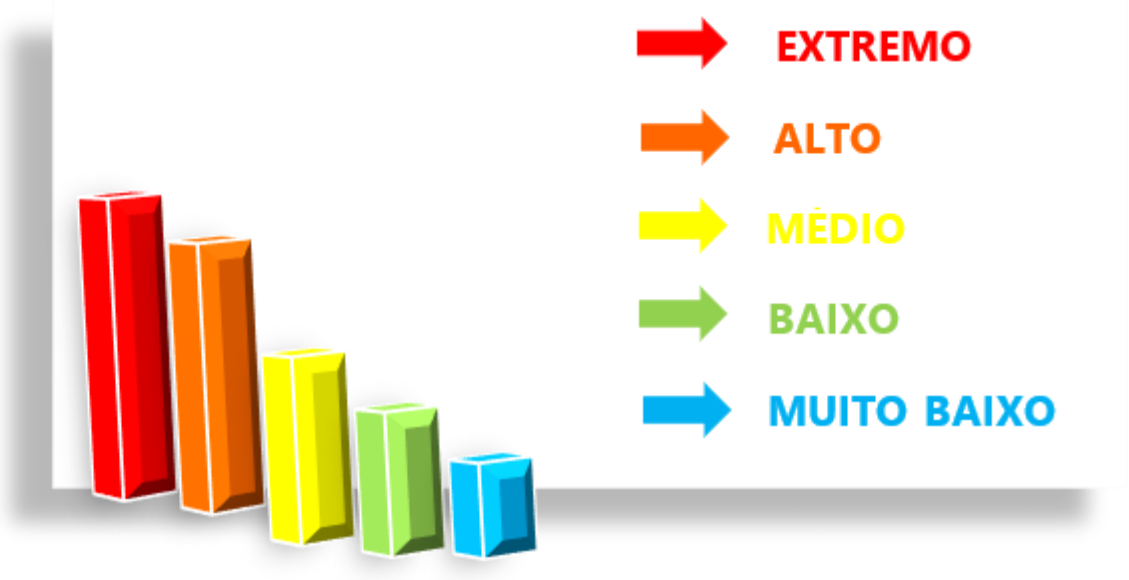
Com vista a aproveitar uma oportunidade

Deve-se implementar as ações de tratamento com os seguintes prazos:



Os riscos considerados muito baixo poderão ser apenas monitorados, a critério do respectivo gestor de riscos.

Níveis de Riscos

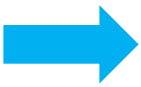


Aqueles caracterizados por riscos associados à paralisação de operações, atividades, projetos, programas ou processos da **Epeople**, causando **IMPACTOS IRREVERSÍVEIS** nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas.

Aqueles caracterizados por riscos associados à interrupção de operações, atividades, projetos, programas ou processos da **Epeople**, causando **IMPACTOS DE REVERSÃO MUITO DIFÍCIL** nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas.

Aqueles caracterizados por riscos associados à interrupção de operações ou atividades da **Epeople**, de projetos, programas ou processos, causando **IMPACTOS SIGNIFICATIVOS** nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas.

Aqueles caracterizados por riscos associados à degradação de operações, atividades, projetos, programas ou processos da **Epeople**, causando **IMPACTOS PEQUENOS** nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas.



Aqueles caracterizados por riscos associados à degradação de operações, atividades, projetos, programas ou processos da **Epeople**, porém causando **IMPACTOS MÍNIMOS** nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas.

Processo de Gestão de Riscos

a. Comunicação e consulta

Processos contínuos e iterativos que a instituição conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas e outros, com relação ao gerenciamento dos riscos. A comunicação e consulta às partes interessadas são importantes na medida em que elas fazem julgamentos sobre riscos com base em suas percepções. Essas percepções podem variar devido às diferenças de valores, necessidades, suposições, conceitos e preocupações das partes interessadas. Como os seus pontos de vista podem ter um impacto significativo sobre as decisões tomadas, convém que as percepções das partes interessadas sejam identificadas, registradas e levadas em consideração no processo de tomada de decisão.

b. Estabelecimento do contexto

Definição dos parâmetros externos e internos a serem levados em consideração ao gerenciar riscos, e estabelecimento do escopo e dos critérios de risco para a política de gestão.

c. Identificação dos riscos

Etapa através da qual o gestor identifica os eventos que podem afetar os objetivos, podendo ser:

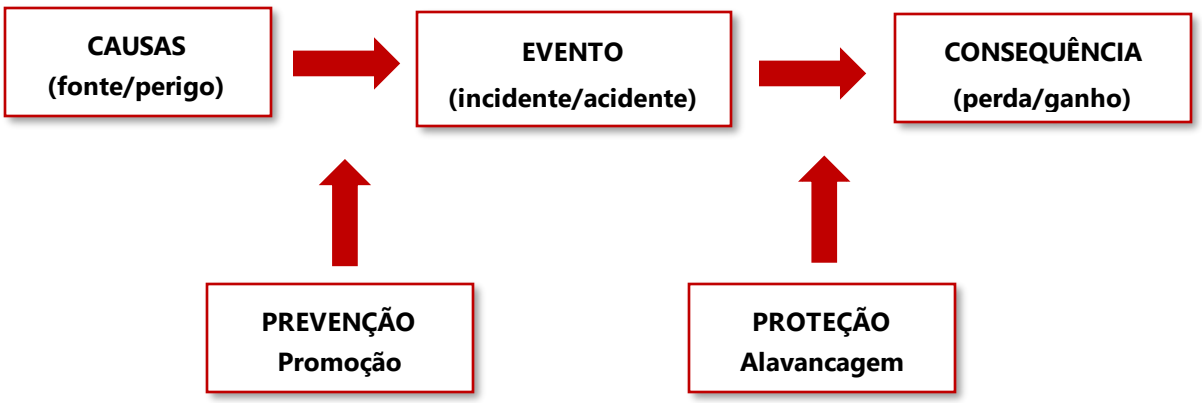
- ✓ riscos positivos (oportunidades); e
- ✓ riscos negativos.

d. Análise dos riscos

É a decomposição dos elementos que formam o risco:

CAUSA (fonte) – EVENTO (sinistro) – CONSEQUÊNCIA (efeito)

Nesta etapa identifica-se a probabilidade de ocorrência do evento, assim como, a sua consequência.



e. Avaliação dos riscos

Etapa através da qual se compara os níveis estimados de risco com os critérios de risco definidos. Nesta etapa o gestor deve lançar os eventos identificados na Matriz de Riscos.

f. Tratamento dos riscos

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar os riscos e a implementação dessas opções. Uma vez implementado fornece novos controles ou modifica os existentes.

Formas de tratamento:

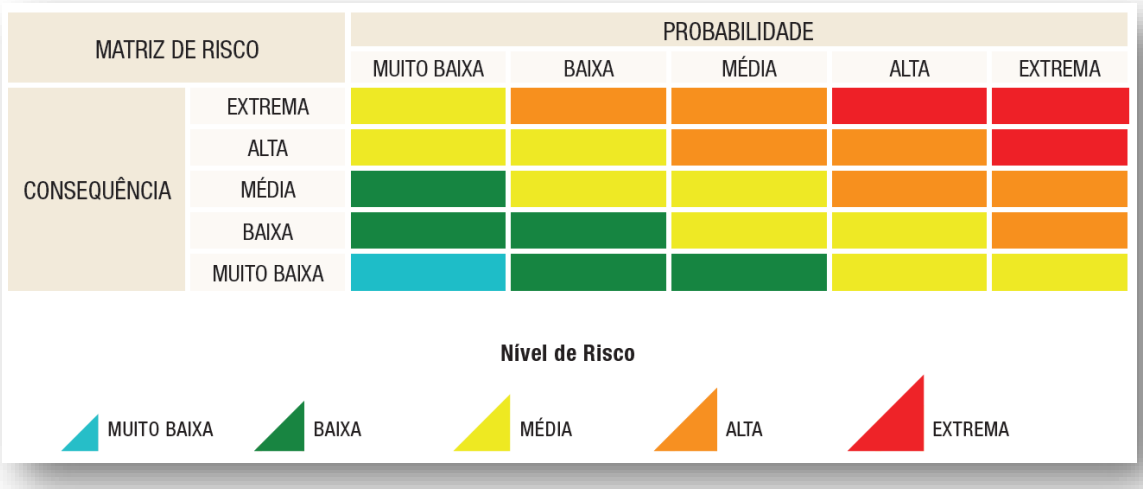
- ✓ evitar o risco;
- ✓ eliminar o risco;
- ✓ reduzir o risco;
- ✓ aceitar o risco;
- ✓ compartilhar o risco; ou
- ✓ aumentar o risco.

g. Monitoramento e análise crítica

Para assegurar que a gestão de riscos seja eficaz e continua a apoiar o desempenho organizacional, convém que o gestor de riscos:

- ✓ meça o desempenho da gestão de riscos utilizando indicadores, os quais devem ser analisados criticamente de forma periódica, para garantir sua adequação;
- ✓ meça periodicamente o progresso obtido, ou o desvio, em relação ao plano de gestão de riscos;
- ✓ analise criticamente de forma periódica se a política, o plano e a estrutura da gestão de riscos ainda são apropriados, dado o contexto externo e interno das organizações;
- ✓ reporte sobre os riscos, sobre o progresso do plano de gestão de riscos e como a de política estão de riscos está sendo seguida; e
- ✓ analise criticamente a eficácia da estrutura da gestão de riscos.

Matriz de Risco



Ferramenta de Avaliação de Risco

BRAINSTORMING

Técnica utilizada para estimular e incentivar o livre fluxo de conversação em equipe, com o objetivo de identificar:

- modos de falha potenciais;
- perigos;
- riscos;
- critérios para decisões;
- opções de tratamento.

ENTREVISTAS ESTRUTURADAS E SEMIESTRUTURADAS

Na entrevista estruturada, há questões elaboradas a partir de uma folha de indicações que incentiva o entrevistado a identificar os riscos a partir de uma perspectiva diferente.

Na entrevista semiestruturada, é permitida mais liberdade para uma conversação e exploração de questões que surgem.

CHECKLIST

Listas de perigos, riscos e falhas de controle ou tratamento desenvolvidas pela experiência (falhas passadas ou avaliações anteriores).

TÉCNICA DE DELPHI

É uma técnica não interativa em que um grupo de especialistas se reúnem para obter consenso a respeito dos riscos de um projeto, processo ou produto.

TÉCNICA DE ESTRUTURA DE WHAT-IF

Exame sistemático em equipe para identificação de riscos de desvios a partir de palavras ou frases de comando - "E se?" - por uma facilitador.

ANÁLISE DE CENÁRIOS

É o desenvolvimento de modelos descritivos de como o futuro poderá se revelar e permite identificar os riscos nesses cenários.

ANÁLISE DE MODOS DE FALHA E EFEITOS - FMEA

Técnica utilizada para identificar as formas em que componentes, sistemas ou processos podem falhar em atender sua intenção de projeto.

ANÁLISE DE ÁRVORE DE FALHAS - FTA

Permite identificar e analisar os fatos que podem contribuir para um evento indesejado.

Os fatores causais são organizados de uma maneira lógica e representados em um diagrama de árvore que descreve também sua relação lógica para o evento de topo.

ANÁLISE DE ÁRVORE DE EVENTOS - ETA

É uma técnica gráfica para representar as sequências mutuamente excludentes de eventos após um evento iniciador, de acordo com o funcionamento, ou não, dos vários sistemas projetados para mitigar as suas consequências.