TERMOS E DEFINIÇÕES

Método Total Risk

Os termos e definições apresentados a seguir foram utilizados no livro Gestão de Riscos na Segurança Patrimonial – www.consultoriadeseguranca.com.br – e no método de avaliação de riscos Total-Risk. É recomendada consulta às normas ABNT ISO GUIA 73 e ABNT NBR ISO 31000, que serviram de referência para o desenvolvimento desta lista.

As definições aqui contidas não visam concluir nem exaurir os temas abordados no livro, e sim servir de mola propulsora para que novas definições, mais completas e adequadas, possam ser desenvolvidas no futuro.

1. **Ambiente externo ou contexto externo:** Características e informações relacionadas ao ambiente externo do sistema de referência estudado. Contexto no qual a organização desenvolve suas atividades e busca atingir seus objetivos. De forma concreta, inclui ruas, bairros, cidade e país. De forma abstrata, envolve cultura, costumes, sociedade, política, leis, economia, maturidade tecnológica e economia.
2. **Ambiente interno ou contexto interno:** Ambiente em que o sistema de referência está inserido. Envolve de forma concreta toda a estrutura física e lógica da organização e de forma abstrata pessoas, cultura organizacional, processos internos, atividades desenvolvidas na organização, estrutura organizacional, funções, responsabilidades, políticas, estratégias, objetivos, sistemas de informação e processo para toma da decisão (formal e informal).
3. **Ameaça**: É qualquer anúncio, ato, indicação, circunstância, perigo ou evento com potencial de prejudicar, amedrontar, causar dano, gerar perdas, consequências negativas ou incerteza nos objetivos da organização. A ameaça é um dos componentes do risco. Na ABNT ISO GUIA 73:2009, os termos *fonte de risco* e *evento* têm significados aproximados ao usado neste livro para ameaça.

4. **Análise de riscos**: Atividade intrínseca ao processo de avaliação de riscos destinada à explicação de como o risco se apresenta em um determinado sistema de referência (organização). Ocorre após a identificação dos riscos e fornece os dados necessários para a próxima seguinte, a avaliação de riscos propriamente dita. É nesta etapa que se quantificam e qualificam o risco e suas variáveis (ameaça, vulnerabilidade, probabilidade, impacto e controles), fornecendo estimativas confiáveis para a avaliação de riscos. As estimativas produzidas durante a análise de riscos servirá de parâmetro de comparação para futuras avaliações de risco.
5. **Ativo**: São os bens e direitos que a empresa possui em dado momento. Pode ser representado por qualquer equipamento, infraestrutura, material, informação, bens tangíveis, bens intangíveis ou atividades que tenham valor para seu proprietário. Para efeito didático, classificamos os ativos em três categorias: ativos físicos (exemplos: carro, computador, edifício etc.); ativos imateriais (exemplos: informação e imagem); e ativos intelectuais (exemplos: funcionários e pessoas que trabalham diretamente nos processos da organização).
6. **Avaliação de risco**: Processo que consiste em comparar os resultados da análise de riscos com os critérios de risco para o determinar se o risco ou sua magnitude é aceitável ou tolerável. A avaliação de riscos deve auxiliar positivamente no processo de tomada de decisão sobre o implantação ou adequação dos controles (tratamento do risco).
7. **BIA (*Business Impact Analyzes*)**: A análise de impacto nos negócios visa identificar, mapear e analisar os processos críticos da organização (incluindo os recursos necessários), a extensão dos eventuais danos, a evolução do impacto no tempo (horas, dias e semanas de inatividade) e os prejuízos decorrentes da ruptura dos processos de negócios. Também é avaliado o custo para retorno à normalidade, o que leva à atribuição de objetivos de recuperação e à priorização.
8. **Ciências atuariais** – Área do conhecimento que dá suporte ao cálculo do valor de seguros, pensões, aposentadorias etc. Têm a base conceitual em ciências como economia, contabilidade, matemática, administração e finanças.
9. **Comunicação**: Ato, efeito ou processo de transmitir e receber mensagens de forma ininterrupta e estruturada. Deve ser interativa e bidirecional. Na segurança, visa

fornecer, compartilhar ou obter dados, informes e informações de interesse dentro das atividade de gestão. As informações podem se referir a contexto, ameaças, vulnerabilidades, consequências, natureza, probabilidade, avaliação, aceitabilidade, controle, tratamento ou outros aspectos da gestão da segurança. Deve subsidiar as decisões por meio da influência e não da imposição pelo poder. O processo de comunicação deve contribuir para a tomada de decisão, e não ser a tomada de decisão coletiva. São os componentes da comunicação: áreas emissoras, receptores, mensagens, canal de propagação, meio de comunicação, resposta e ambiente no qual o processo comunicativo se realiza. O processo de comunicação sofre interferências devidas a ruído, interpretação, compreensão e contexto.

10. **Consequência**: Resultado percebido após a materialização de um risco. É o impacto percebido após uma ameaça explorar vulnerabilidade da organização. Efeito negativo ou positivo de um evento que afeta os objetivos da organização. Um evento pode gerar mais de uma consequência e uma consequência pode gerar um ou mais eventos. As consequências podem ser expressas de forma quantitativa e qualitativa. Também pode ser usado o termo impacto.
11. **Crise**: Situação aflitiva, momento grave, conjuntura perigosa, dificuldades graves. A crise pode gerar consequências, necessidade de adaptações rápidas e desequilíbrio na organização ou seus processos. A evolução da crise pode trazer benefícios ou perdas à organização, dependendo da velocidade, eficácia e eficiência da resposta. Toda crise conduz necessariamente ao aumento da vulnerabilidade, maior exposição à ameaças, e requer capacidade de adaptação e de reação. No campo da psicologia, em particular da psicologia do desenvolvimento, o conceito de crise é explicado como toda a situação de mudança biológica, psicológica ou social, exigindo da pessoa ou grupo esforço suplementar para manter equilíbrio ou estabilidade emocional. Corresponde a momentos da vida de uma pessoa ou de um grupo em que há ruptura na sua homeostase psíquica e perda ou mudança dos elementos estabilizadores habituais.
12. **Critérios de risco**: Referência utilizada como parâmetro para o processo de avaliação de risos em uma organização. Para definir os critérios de risco são levados em consideração os fatores críticos de sucesso da organização, os objetivos da

organização, o contexto interno e o contexto externo. Podem influenciar os critérios de riscos: cultura organizacional, cultura do país ou região, normas, políticas, leis, entre outros.

13. **Decisor, tomador de decisão ou cliente-decisor**: Neste trabalho utilizamos essa terminologia para nos referir ao presidente, CEO, executivo responsável ou simplesmente o cliente-contratante do serviço de consultoria ou projeto de segurança. Estamos nos referindo ao profissional da organização com responsabilidade para contratar os serviços de segurança, decidir sobre que ações deverão ser desenvolvidas em resposta às informações obtidas por meio da avaliação de riscos. Normalmente esse profissional também será o detentor ou proprietário dos riscos avaliados.
14. **Estratégia de tratamento do risco**: Abordagem da organização para avaliar os riscos e eventualmente definir formas de tratamento para modificá-los por meio de adequação dos controles existentes ou implantação de novos controles. As possíveis atitudes da organização perante o risco são: assumir (aceitar), compartilhar, financiar (agir na consequência), afastar-se ou evitar o risco. No mercado também existem outras nomenclaturas para designar essas possíveis atitudes perante o risco. Buscar e reter também são atitudes possíveis perante o risco, porém, pouco encontradas na segurança patrimonial. O processo de tratamento do risco pode envolver uma das ações a seguir ou uma combinação delas: alteração da probabilidade, do impacto, controle da ameaça ou redimensionamento das vulnerabilidades. A estratégia de tratamento do risco também pode ser referenciada como mitigação do risco, prevenção de risco ou atitude perante o risco.
15. **Estrutura de gestão da segurança**: conjunto de processos, pessoas e atividades que fornecem as bases organizacionais para estudos, projetos, implementação, monitoramento, análise crítica e melhoria contínua da estrutura de gestão da segurança em toda a organização. As bases da estrutura incluem a estratégia, objetivos, política, recursos envolvidos, responsabilidades, processos e atividades. A estrutura de gestão da segurança deve estar presente em todas as áreas, processos, atividades e locais da organização.

16. **Evento ou evento de risco**: Ocorrência, ausência de ocorrência ou mudança em um conjunto específico de circunstâncias com ou sem impacto para a organização. Um evento de risco pode ter várias causas de origens diferentes, geradas por fatores: humano (proveniente de ação - ou omissão do ser humano - direta ou indiretamente, voluntária ou involuntariamente); natural (proveniente de fenômenos da natureza); técnico (oriundo de falha ou emprego inadequado de equipamentos, utensílios ou instrumentos); e biológico (causado por animais ou microrganismos).
17. **Fatores críticos de sucesso**: Os fatores críticos de sucesso (FCS) são critérios que podem definir o sucesso ou o fracasso de um ou mais objetivos definidos no planejamento estratégico de determinada organização. Os FCS podem ser considerados diferenciais na definição das estratégias que serão adotadas pela organização e da necessidade que estas têm de satisfazer o cliente por meio desses fatores. Os FCS são identificados mediante estudo a respeito dos próprios objetivos da organização ou derivados deles, e estabelecidos como condições fundamentais a serem cumpridas para que a instituição sobreviva e prospere. Quando bem definidos, os FCS tornam-se referências para as atividades da organização.
18. **Gerenciamento de crise**: Atividade atípica com objetivo de identificar, obter e aplicar processos específicos e recursos estratégicos para a solução de crises. Estabelece ações e responsabilidades pela condução do processo. Deve ser previamente desenvolvida e revisada periodicamente para manter-se eficaz e evitar consequências que possam se originar deem eventos de risco intrínsecos às atividades da organização. Caracteriza-se pelo estado de grandes tensões, com elevada probabilidade de agravamento, difícil previsão de desdobramentos e extensão.
19. **Gestão de riscos**: Ações ou processos coordenados para conduzir e controlar uma empresa ou organização em tudo que seja relacionado a riscos. Também pode ser descrito como gestão dos riscos de segurança para designar objetivamente que parte dos riscos da organização serão gerenciados.
20. **Identificação de riscos**: Atividade estruturada e coordenada que visa reconhecer, localizar, apontar, entender, nomear, distinguir e diferenciar os riscos de uma

organização e seus componentes (ameaça, vulnerabilidade, probabilidade, impacto e controles). O processo de identificação de riscos pode evolver (sem se limitar a) observações, entrevistas e testes comprobatórios (experimentos).

21. **Impacto**: O mesmo que consequência, resultado de um evento de risco que afeta os objetivos da organização. O impacto é um dos componentes do risco.
22. **Impacto financeiro**: Conversão e somatória em valores monetários de todas as consequências diretas (ou intrínsecas), indiretas (ou subjetivas), advindas da materialização de um risco ou grupo de riscos.
23. **Inspeção**: Ato ou efeito de inspecionar, vistoriar, fiscalizar.
24. **Manual de segurança**: Conjunto de normas, regulamentos e procedimentos de segurança agrupados em um mesmo caderno, apostila, livro ou arquivo informático, organizado em ordem determinada pelo responsável por seu cumprimento, com objetivo de disciplinar a a execução de atividades de segurança dentro dos microprocessos e no macroprocesso da organização.
25. **Método**: Em ciência, o método é constituído por uma série de passos codificados para serem seguidos de forma mais ou menos estruturada a fim de se atingir determinado objetivo científico. Podemos entender método como: Maneira de dizer, de fazer, de ensinar uma coisa, segundo certos princípios e em determinada ordem. Maneira de agir. Busca racional de explicações: método cartesiano. Sinônimos de método: arrumação, maneira, ordem, processo e sistema. Para os objetivos deste trabalho, nos referimos ao método de trabalho, ou simplesmente método, para denotar a forma como uma atividade de consultoria é organizada, estruturada e desenvolvida.
26. **Metodologia**: Deve-se notar que a palavra metodologia é muitas vezes usada quando seria mais adequada a palavra método. O termo metodologia inclui os seguintes conceitos, em relação a uma disciplina particular ou campo de estudo: coleção de teorias, conceitos e ideias; estudo comparativo de diferentes enfoques ou métodos; e crítica a um método individual. A metodologia é o estudo dos métodos. Tem como objetivo captar e analisar as características de vários métodos, avaliar suas capacidades, potencialidades, limitações ou distorções e criticar os pressupostos ou as implicações de sua utilização, além de ser uma disciplina que

estuda os métodos, a metodologia é a explicação minuciosa, detalhada, rigorosa e exata de toda ação desenvolvida no método (caminho) do trabalho de pesquisa.

27. ***Modus operandi***: Expressão em latim que significa "modo de operação". Significa a maneira de agir ou executar uma atividade, normalmente realizada sempre da mesma forma, possibilitando identificar quem a realizou.
28. **Normas de segurança**: Regulamentam e fornecem orientações sobre procedimentos de segurança obrigatórios relacionados a uma organização. Podem estar agrupadas por tema ou por assuntos correlatos, organizados em ordem determinada pela organização sobre sua aplicabilidade.
29. **Organização**: Para efeito deste estudo, consideramos organização qualquer empresa privada, pública, comunitária, associação, grupo de pessoas ou mesmo um indivíduo. Não está limitada a setor ou área de atividade.
30. **Plano de continuidade de negócio**: do inglês *Business Continuity Plan* – BCP, estabelecido pela norma ABNT NBR 15999 Parte 1, é o desenvolvimento preventivo de um conjunto de estratégias, planos de ação e atividades visando garantir que os serviços essenciais sejam identificados e preservados após ocorrência de desastre, até retorno à normalidade. O plano de continuidade de negócios é responsabilidade dos dirigentes da organização. É constituído pelos seguintes planos: plano de contingência; plano de administração de crises (PAC); plano de recuperação de desastres (PRD); e plano de continuidade operacional (PCO). Esses planos visam formalizar ações a serem desenvolvidas em momentos de crise, recuperação, continuidade e retomada, evitando que os processos críticos de negócio da organização sejam afetados e acarretem perdas financeiras.
31. **Plano de gestão da segurança**: Forma, maneira, sequência de atividades dentro da estrutura de gestão da segurança que especifica a abordagem, os componentes de gestão e os recursos humanos, técnicos e organizacionais a serem utilizados para gerenciar a segurança frente aos riscos identificados na organização. O plano pode incluir normas, procedimentos, controles, atividades, ações, práticas, atribuições, responsabilidades, passos a serem seguidos, cronologia das atividades e pode ser aplicado a parte de um processo, departamento, estrutura física ou a toda organização.

32. **Plano de recuperação de desastre (ou *Disaster Recovery Plan* – DRP)**: processo documentado indicando responsabilidades e ações a serem realizados para recuperar serviços e processo críticos de uma organização após eventos extremos com parada total ou parcial de suas atividades e processos. Visa o retorno à normalidade no mais curto espaço de tempo, minimizando consequências que possam levar ao desaparecimento da organização. O planejamento é composto por várias fases e pode prever as seguintes etapas: planejamento inicial das atividades; avaliação de vulnerabilidade e definição de exigências da organização ou projeto; identificação, análise e avaliação de consequências ao negócio; detalhamento das consequências em diversos cenários; desenvolvimento do plano propriamente dito; plano de simulação; plano de manutenção e atualização; e implantação.
33. **Plano de emergência**: Sistematização de conjunto de normas, procedimentos lógicos, técnicos e administrativos, estruturados para minimizar ou evitar consequências resultantes de catástrofes previsíveis como incêndio. Por meio da gestão eficiente dos recursos disponíveis, propicia resposta rápida e eficaz. Visa proteger a vida, o meio ambiente e ativos da organização, bem como contribuir para a continuidade dos negócios. Fornece informações técnicas e operacionais sobre a estrutura física da organização e suas áreas críticas.
34. **Política de gestão da segurança**: Declaração da organização contendo suas intenções e diretrizes gerais relacionadas aos riscos envolvidos em suas atividades e como serão tratados pela estrutura de gestão da segurança.
35. **Premissas ou contexto**: Identificação e estabelecimento das variáveis internas e externas de risco relativos a um sistema de referência (organização). Normalmente identificados e definidos a partir de levantamentos de campo, entrevistas, pesquisas e investigações diversas. São necessários para estabelecer o escopo do trabalho relacionado à gestão da segurança e aos critérios de risco que serão utilizados no processo de avaliação de risco.
36. **Probabilidade**: É a possiblidade ou chance de algo (evento incerto ou conhecido) vir a ocorrer, não importando se é possível medir, definir ou determinar. A probabilidade, quando relacionada ao risco, pode ser descrita e definida de forma objetiva ou subjetiva, qualitativa ou quantitativa, usando-se termos gerais ou

matemáticos. Em termos matemáticos, a probabilidade varia entre 0 (impossível de ocorrer) e 1 (certeza inequívoca de algo correr). A probabilidade é um dos componentes do risco. Dependendo do contexto utilizado, a palavra probabilidade pode aparecer como possibilidade, viabilidade, expectativa, risco, incerteza, dúvida, pressuposição, sorte, esperança ou azar.

37. **Procedimentos de segurança**: Maneira de agir, sequência de ações ou instruções a serem seguidas para resolver problemas e efetuar tarefas relacionadas à segurança.
38. **Processo de avaliação de riscos**: Processo completo e abrangente que envolve identificação, análise riscos e avaliação de riscos de um sistema de referência (organização). Faz parte do processo de gestão da segurança de uma organização.
39. **Processo de gestão de riscos**: Trata-se de um processo estruturado que amplia o processo de avaliação de risco para permitir a atividade de gestão. Para entendimento completo consultar, ABNT ISO GUIA 73:2009.
40. **Processo de gestão da segurança**: aplicação sistemática de políticas, normas, procedimentos e práticas de administração para as atividades de gestão da segurança na organização. Também envolve as atividades de gestão de riscos.
41. **Processo de tomada de decisão**: processo cognitivo pelo qual se escolhe uma estratégia e um conjunto de ações, dentre várias opções, com base em avaliações de risco, cenários, ambientes, opiniões, estudos e outros fatores. O processo decisório deve produzir obrigatoriamente uma escolha final, ou seja, a tomada de decisão refere-se ao processo de escolher o caminho mais adequado à empresa, em uma determinada circunstância.
42. **Projeto**: A palavra projeto vem da palavra latina *projectum* do verbo latino *proicere*, "antes de uma ação", que por sua vez vem de pró-, que denota precedência, algo que vem antes de qualquer outra coisa no tempo (em paralelo com o grego πρό) e iacere, "fazer". Portanto, a palavra "projeto", na verdade, significava originalmente "antes de uma ação". São estas as principais características dos projetos: são temporários, com início e fim definidos; são planejados, executados e controlados; entregam produtos, serviços ou resultados únicos; são desenvolvidos em etapas e continuam por incremento com elaboração progressiva; são realizados por pessoas; e têm recursos limitados. O Guia PMBOK, um guia em gerenciamento de projetos, é

amplamente reconhecido como boa prática e utilizado como base pelo *Project Management Institute* (PMI). Esse mesmo guia identifica seus elementos recorrentes no gerenciamento de projetos, que são cinco: Início; planejamento; execução; monitoramento e controle; e encerramento. Dez são as áreas gerenciadas nos projetos: integração; escopo; custos; qualidade; aquisições; recursos humanos; comunicações; risco; tempo; e partes interessadas. Neste trabalho, nos referimos ao projeto como qualquer atividade desenvolvida pelo consultor com as seguintes características principais: ser temporária, ter início e fim definidos; ser planejada, executada e controlada; entregar serviço ou resultado únicos; ser desenvolvida em etapas; e ter recursos definidos e controlados.

43. **Proteger**: Defender, preservar, resguardar, abrigar ou amparar do evento de risco as pessoas, bens, informações e imagem. A proteção muitas vezes está relacionada à contenção de ameaça ou redução da vulnerabilidade existente.
44. **Recursos de segurança ou controles de segurança**: são todas as atividades, práticas, ações, processos, procedimentos, equipamentos, tecnologias, normas, políticas ou medidas capazes de modificar os riscos da organização. Didaticamente, os recursos de segurança são divididos em: humanos, técnicos e organizacionais. Têm por objetivo proteger ativos e pessoas da organização contra ameaças, reduzindo vulnerabilidades ou probabilidade, ou ainda limitando consequências indesejáveis.
45. **Redução do impacto**: Controle da extensão das consequências que determinado risco pode produzir.
46. **Risco**: Efeito (positivo ou negativo) da incerteza nos objetivos, podendo ocasionar desvios. O risco tem como variáveis: ameaça, vulnerabilidade, probabilidade, impacto e controles. O risco é intrínseco às atividades humanas e só é possível ser eliminado completamente quando encerrada(s) a(s) atividade(es) correspondente(s). Os riscos podem ser classificados de diversas formas e com distintos critérios. Uma das formas mais utilizadas para se verificar a magnitude ou o nível de um risco considera a combinação do impacto (consequência) e da probabilidade.
47. **Risco residual**: Um risco não pode ser eliminado sem se eliminar também a atividade envolvida. Portanto, o tratamento de todo risco, com a finalidade de trazê-lo para níveis aceitos pela organização, pressupõe riscos residuais. Todo risco remanescente

após ter sido devidamente tratado pode ser considerado risco residual ou risco retido.

48. **Segurança**: Estado, qualidade, condição daquilo que se percebe seguro, isento de perigo, acautelado, protegido. Percepção, sensação ou sentimento de estar protegido de riscos, perigos, perdas, ameaças ou consequências. A sensação da segurança pode percebida de forma distinta pelas partes interessadas dentro de um mesmo projeto, departamento ou organização.
49. **Segurança corporativa**: Também conhecida como segurança institucional, segurança empresarial ou segurança da organização. Visa tratar eventos de riscos e suas variáveis – ameaça, vulnerabilidade, probabilidade, impacto e controles – por meio de processos que envolvem recursos humanos, técnicos e organizacionais com o objetivo de diminuir as incertezas nos objetivos da organização. Protege pessoas, bens, informações, imagem e meio ambiente. Utiliza técnicas apropriadas, buscando equilíbrio entre investimento, proteção e nível de riscos, sempre com foco nos objetivos da organização e seus fatores críticos de sucesso.
50. **Sensação de insegurança (ou percepção de risco)**: Percepção, sensação, visão ou sentimento de que algo possa acontecer, produzindo consequências diferentes das esperadas. Aumento do efeito negativo da incerteza nos objetivos da organização.
51. **Sinistro**: Ocorrência já materializada que impacta, causa dano, prejuízo, perda, sofrimento ou morte. O sinistro é resultado de um ou mais eventos com consequências negativas (exemplos: incêndio, acidente, roubo, furto etc.) para a organização ou pessoa.
52. **Sistema de referência (SR)**: Para efeito deste estudo, consideramos sistema de referência toda ou parte de uma empresa privada, pública, comunitária, associação, grupo de pessoas ou indivíduos. Não está limitada a setor ou área de atividade. A diferença didática entre a definição de organização e sistema de referência é que o segundo pode estar limitado a uma instalação, pessoa, processo, projeto, ativo, fração, parte ou atividade de uma organização. O SR é o objeto ou objetivo a partir do qual se dsenvolve a avaliação de risco.

53. **SLA** *(service level agreement):* Acordo de nível de prestação de serviço para o controle efetivo dessa qualidade na prestação de serviços. Pode se referir a um processo ou a toda a organização.
54. **Vulnerabilidade**: Características intrínsecas de uma organização, processo, atividade ou objeto resultando em suscetibilidade a uma ou mais ameaças que podem levar a um sinistro (ou acidente) com um impacto. Debilidade, predisposição ou fragilidades intrínsecas a uma organização, estrutura ou equipamento resultando em suscetibilidade a uma ameaça (fonte de risco), possibilitando acesso a bens ou pessoas, podendo vir a causar consequências, danos ou perdas (impacto). Organizações distintas têm níveis de exposição também distintos para as mesmas vulnerabilidades. A vulnerabilidade é um dos componentes do risco.