Análise de Risco de Pessoa: a Convergência das Medidas de Proteção Com os Procedimentos de Segurança Adequados

PERSONAL RISK ANALYSIS: THE CONVERGENCE OF PROTECTION MEASURES WITH SECURITY PROCEDURES

ANÁLISE DE RISCO DE PESSOA: A CONVERGÊNCIA DAS MEDIDAS DE PROTEÇÃO COM OS PROCEDIMENTOS DE SEGURANÇA ADEQUADOS

PERSONAL RISK ANALYSIS: THE CONVERGENCE OF PROTECTION MEASURES WITH SECURITY PROCEDURES

Felipe Scarpelli de Andrade[1]
Alessandre Roberto dos Reis[2]
Marcelo Couto Sanches[3]

RESUMO

A abordagem tradicional voltada para a segurança pessoal é traduzida por um conjunto de medidas preventivas que visam proteger uma pessoa de potenciais ameaças. Entretanto, não há um planejamento quanto à conformidade do nível de proteção que uma pessoa requer em função do risco identificado. Nesse contexto, o objetivo deste estudo é apresentar uma estrutura de análise de risco que permita auxiliar, de forma metodológica e com foco no risco, o planejamento da proteção individual de determinado indivíduo, a fim de trazer harmonia aos procedimentos ao relacioná-los com as vulnerabilidades e as potenciais ameaças. Dessa forma, para uma proteção adequada, entende-se que a análise de risco é instrumento fundamental para o planejamento da segurança pessoal, ao possibilitar compreender os elementos que são influenciados e podem influenciar na concretude de um evento indesejado. Ao contemplar um estudo com base em risco, este trabalho propõe uma metodologia de Análise de Riscos de Pessoa (ARP) que permite abordar os problemas relacionados à incerteza, a fim de buscar a convergência dos procedimentos de segurança a uma atuação preventivamente equilibrada, na medida em que reduz a possibilidade de ineficácia ou insuficiência das medidas de segurança implementadas pela abordagem tradicional. Trata-se, portanto, da modelagem de uma estrutura sistematicamente disciplinada, voltada para a avaliação e a melhoria da eficácia dos processos de proteção pessoal.

Palavras-chave: análise de risco; segurança pessoal; medidas de proteção; proteção de autoridade.

ABSTRACT

The traditional approach aimed at personal security is a set of preventive measures focused at protecting a person from potential threats. However, there is no planning as to the adequacy of the level of protection that a person requires due to an identified risk. In this context, the objective of this study is to present a risk analysis structure that allows to help, in a methodological way and with a focus on risk, the planning of the individual protection of a given individual, in order to bring suitability to the procedures in accordance with vulnerabilities and potential threats. Thus, for adequate protection, it is understood that risk analysis is a fundamental tool for planning personal safety, as it makes it possible to understand the elements that are influenced and can influence the concreteness of an unwanted event. By contemplating a risk-based study, this work proposes a methodology of Person Risk Analysis (PRA), which allows addressing the problems related to uncertainty, and assists the convergence of security procedures for a preventively balanced action, as it reduces the possibility of ineffectiveness or insufficiency of the security measures implemented by the traditional approach. It is, therefore, the modeling of a framework that processes data in an analytical way and provides systematically disciplined knowledge for evaluating and improving the effectiveness of personal protection processes.

Keywords: risk analysis; personal security; protective measures; authority protection.

Data de submissão: 27/08/2021 – Data de aprovação: 03/06/2022

1 Mestre em Gestão de Riscos pela UFPE. Agente de Polícia Federal. Professor e conteudista da Academia Nacional de Polícia e da Secretaria de Gestão e Ensino em Segurança Pública.
2 Especialista em Ciências Policiais. Agente de Polícia Federal. Professor da Academia Nacional de Polícia e da Secretaria de Gestão e Ensino em Segurança Pública.
3 Graduado em Tecnologia de Sistemas da Informação. Perito Criminal da Polícia Civil do Rio de Janeiro. Coordenador de Análise de Riscos SEPOL-RJ.

1. INTRODUÇÃO

O trabalho de segurança pessoal, entendido como aquele que visa a adotar um conjunto de ações de natureza preventiva para preservar e assegurar a integridade física de um indivíduo não considera, de uma forma geral, a necessidade de um planejamento operacional com foco no risco.

A abordagem tradicional, em que os meios para uma segurança pessoal são uma função direta com a quantidade de efetivo para proteção, treinamento, uso de armamentos, veículos blindados e equipamentos, deve aprimorar-se. Isto é, dispositivos e recursos a serem adotados nos diversos locais em que um dignitário ou autoridade esteja presente ou percorre, como residência, trabalho, deslocamentos, eventos públicos ou ambientes sociais, requerem um estudo orientado com base no risco, a fim de trazer adequabilidade aos procedimentos em conformidade com as vulnerabilidades e as potenciais ameaças.

Portanto, parte-se da premissa de que a falta de uma abordagem orientada pelo risco, que envolva a identificação, análise e avaliação da exposição de uma determinada pessoa a ser protegida, conduz à ineficácia ou insuficiência das medidas de segurança implementadas (ANDRADE; ROCKEMBACH, 2018). Analisar os métodos de segurança adequados para a atividade de proteção de pessoas, bem como o perfil dos agentes que atuam nessa área não são suficientes: a proteção pessoal deve ser planejada de forma que haja uma correlação entre as medidas preventivas e os riscos identificados.

O objetivo deste estudo é apresentar uma modelagem básica de Análise de Risco de Pessoa que permita auxiliar, de forma metodológica e com foco no risco, o planejamento da proteção individual de um determinado indivíduo. A convergência dos procedimentos de segurança com a análise de riscos é elemento fundamental para auxiliar a tomada de decisão no emprego de controles preventivamente equilibrados.

2. REFERENCIAL TEÓRICO

O termo "segurança" remete-nos à ideia de uma situação em que haja isenção de riscos. Todavia, a eliminação completa de todos os riscos é impossível, uma vez que a incerteza está presente em distintos aspectos humanos, como segurança das instalações, processos, meio ambiente, social, operacional, estratégico, entre outros. Com efeito, a segurança passa a ser um compromisso acerca de uma relativa proteção da exposição a riscos (PORTELLA, 2004).

A palavra "risco" notabilizou-se, na última metade do século passado (WILLIAMS, 1985), quando militares, organizações civis, pesquisadores, especialistas, políticos, editores e diversas instituições perceberam a necessidade de se enfrentar de maneira mais sistemática os problemas relacionados à incerteza (RENN, 2008).

A partir de então, com a pesquisa e evolução dos métodos, algumas definições sobre risco foram criadas, como: "a incerteza de resultado de ações e eventos" (UNITED KINGDOM, 2013, p. 40, tradução nossa); "a possibilidade de que um determinado evento indesejável ocorra" (COSO II, 2004, p. 16, tradução nossa); "possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos" (BRASIL, 2016, p. 2); "efeito da incerteza nos objetivos" (ISO 31000, 2018, p. 1). Tradicionalmente, o risco é definido como uma correlação da probabilidade e do impacto de ocorrência de um evento (AVEN, 2015).

A Análise de Riscos (AR), por sua vez, é um processo de identificação e avaliação de riscos, cujo propósito é apoiar decisões, independentemente de suas fontes estarem ou não sob o controle do usuário. Já o tratamento efetivo do risco, isto é, a sua administração, depende da racionalização da estrutura provida pela AR para aumentar a capacidade de se distinguirem opções em um contexto mais bem estruturado (ANDRADE, 2019). Trata-se da Gestão de Riscos (GR).

A despeito de haver distintas metodologias de AR desenvolvidas por pesquisadores nos meios acadêmico e corporativo, a modelagem de uma estrutura deve ser personalizada (ISO 31000, 2018) consoante o seu propósito, ou seja, o processo depende da declaração do objetivo da análise ou do contexto definido.

Dessa forma, ao considerar que a finalidade da segurança pessoal é proporcionar proteção a determinada autoridade, convém que as ações preventivas sejam planejadas e orientadas não apenas em protocolos descritivos de proteção, mas pautadas em uma análise de riscos que considera importantes elementos nesse contexto, como as vulnerabilidades e as potenciais ameaças. Essa abordagem permite melhor relacionar os resultados da análise com os critérios, para determinar qual o procedimento mais adequado em função do risco apresentado.

Nessa esteira, a metodologia de avaliação de risco de pessoa deve considerar que diferentes estruturas são necessárias para distintas situações. Com efeito, a modelagem apresentada pode ser adaptada em todas as abordagens de avaliação de risco que tratam de proteção pessoal.

Uma das diferenças mais notadas entre as várias técnicas de avaliação de risco de segurança é a maneira como as variáveis de decisão de risco são determinadas ou calculadas. Segundo Landoll (2006), as variáveis de decisão incluem pelo menos os seguintes aspectos: o valor do ativo, a probabilidade de que uma vulnerabilidade seja explorada e a gravidade do impacto.

Ainda, a depender das circunstâncias, a análise pode ser qualitativa, quantitativa ou uma combinação destas. Entretanto, qualquer estudo deve considerar dois importantes parâmetros: a mensuração da probabilidade da ocorrência de um risco e, caso se concretize, o impacto potencial que ele geraria no ativo analisado (ANDRADE, 2017).

O método William T. Fine (FINE, 1971) para identificação e avaliação de riscos, por exemplo, é uma ferramenta de análise que tem como objetivo estabelecer prioridades de ação sobre os riscos identificados, ao equacioná-lo com a disponibilidade econômica. A definição da prioridade leva em consideração o grau de criticidade (impacto) dos riscos avaliados.

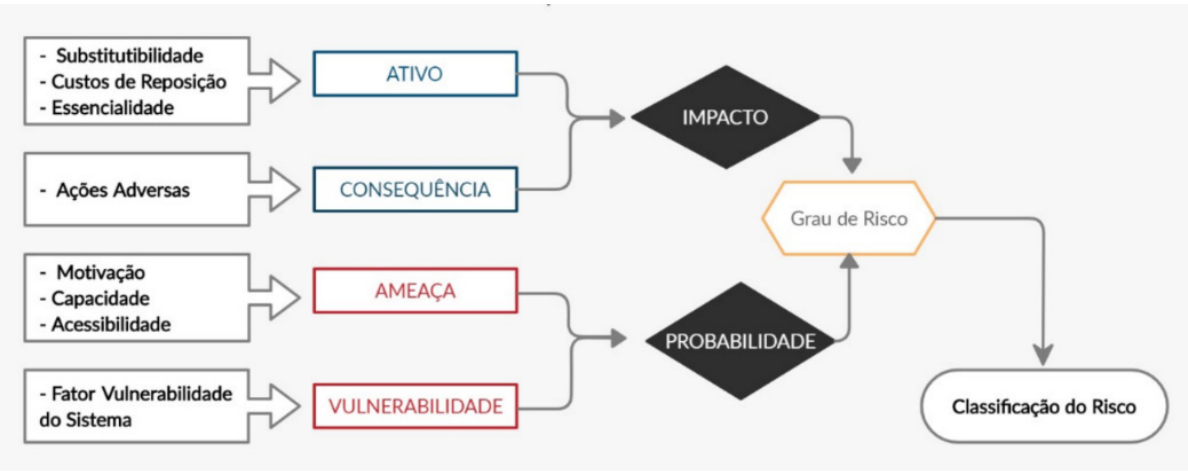
A mesma lógica ocorre com o Método Mosler (RODRÍGUEZ; CONTRERAS, 2014), utilizado para avaliar as ameaças que podem influenciar negativamente as atividades da organização, cuja finalidade, assim como no Método T. Fine, é classificar os riscos de acordo com as suas gravidades.

Como o objetivo aqui é preservar e assegurar a integridade física de um indivíduo, não há negociação quanto à ordem de gravidade, na medida em que a consequência não é uma variável "negociável" neste estudo. Em outras palavras, e considerando que a equação do risco é uma função da probabilidade e do impacto, as análises com foco na proteção de pessoas devem centrar seus esforços com base em variáveis de probabilidade.

A metodologia Análise de Risco em Segurança Orgânica (ARSO), proposta por Andrade e Rockembach (2018), considera igualmente as variáveis probabilidade e impacto. Como reflexo, o processo

dispõe sobre os elementos que, correlacionados, permitem aferir um determinado grau de risco no contexto de instalações físicas, sendo eles os seguintes: ativo, ameaça, vulnerabilidade e consequência (Fig. 1). Trata-se de uma análise qualitativa que depende do julgamento subjetivo de especialistas responsáveis pela avaliação para determinar o risco geral do sistema em estudo.

FIGURA 1 – FLUXOGRAMA DA METODOLOGIA ANÁLISE DE RISCO EM SEGURANÇA ORGÂNICA (ARSO)



Fonte: Elaborado pelos autores, adaptado de Andrade e Rockembach (2018).

A análise qualitativa é usada para qualificar um risco em palavras, ou termos, estabelecendo-se acordos semânticos, enquanto a abordagem quantitativa busca qualificá-lo em uma expressão matemática. A análise semi-qualitativa, por sua vez, procura atribuir valores numéricos aos termos identificados na análise qualitativa, sem que haja a necessidade de que os valores correspondam exatamente à intensidade da probabilidade ou do impacto, isto é, o objetivo é encontrar a região em que as variáveis do risco se encontram, e não os seus valores rigorosamente precisos (ANDRADE, 2019).

Considerando-se a dificuldade da análise quantitativa de mensurar os valores das probabilidades de eventos negativos – como a frequência com que uma ameaça atacou uma determinada pessoa, por exemplo –, devido à limitação de dados disponíveis, a abordagem qualitativa é recomendada para avaliar o risco em segurança pessoal. Isso porque a análise quantitativa depende de dados em quantidade e qualidade tais que seja possível compará-los utilizando técnicas baseadas em estatísticas e em uma análise histórica dos registros de incidentes de segurança, a fim de calcular e interpretar o risco. Esses dados dificilmente seriam obtidos quando o objetivo é a proteção específica de uma determinada pessoa.

Não é conveniente analisar, a partir somente de informações pretéritas, que há ausência de risco de segurança de uma determinada pessoa caso ela não tenha sofrido alguma ação adversa no passado. Neste caso, os dados quantitativos não são suficientes.

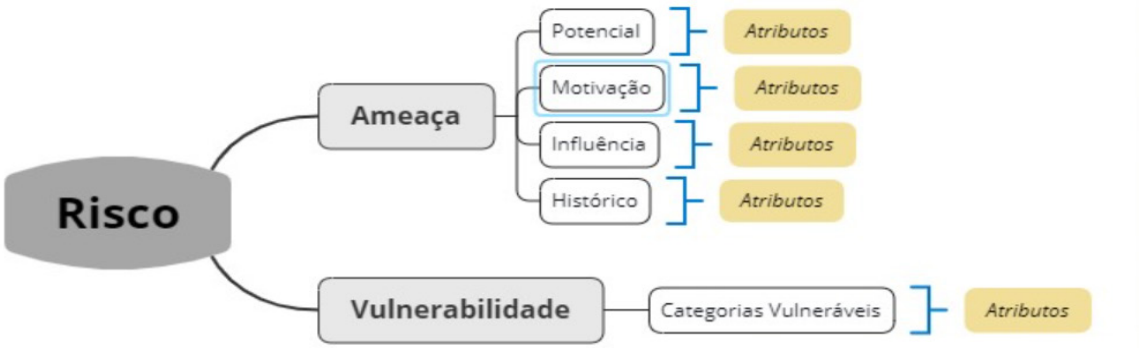
Climaco, Cardoso e Sousa (2004) indicam que os métodos quantitativos tradicionais da Pesquisa Operacional (PO) *Hard* não foram, a partir do fim da década de 1960, capazes de tratar os problemas com crescente complexidade devido ao ambiente interconectado e à falta de dados estatísticos. Como reflexo, a PO *Soft* surgiu para reduzir essas fragilidades, na medida em que dedica especial atenção aos aspectos qualitativos e notadamente subjetivos dos processos de decisão. Essa abordagem apresenta como característica a busca por um aprendizado e a uniformização das informações sobre o problema entre as partes envolvidas, e não a sua otimização (ANDRADE, 2019).

Na terminologia da análise de risco, a palavra probabilidade é utilizada para referir-se à chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ANDRADE, 2019).

O impacto, por sua vez, refere-se à gravidade dos danos potenciais de uma ação hostil, verificada pela quantificação da consequência negativa presumível. Apesar da possiblidade de o impacto processar-se com base em diversos parâmetros, como a confiabilidade da imagem da organização, a sensação de segurança, a repercussão na mídia, o número estimado de perdas em recursos humanos e materiais, o público envolvido, entre outros, a análise de risco proposta neste estudo não considera este elemento como uma variável, já que o potencial impacto – morte, invalidez permanente ou sequestro, por exemplo, não são transacionados.

Dessa forma, ao considerar que a análise de risco de pessoa é uma função da probabilidade de um evento indesejado ocorrer e o subjacente impacto caso ele se materialize, e que este não é uma variável - já que a incolumidade do indivíduo não será negociada -, a construção da metodologia Análise de Rico de Pessoa (ARP) centrará os seus estudos em uma análise semi-qualitativa de probabilidade.

FIGURA 2 – METODOLOGIA ANÁLISE DE RISCO DE PESSOA



Fonte: Elaborado pelos autores (2021).

Do exposto (Fig. 2), tem-se que a mensuração do risco na metodologia ARP é expressa por meio da equação: RISCO = VULNERABILIDADE + AMEAÇA.

As vulnerabilidades são traduzidas pelas características do ambiente interno que facilitam a concretização da ameaça. Trata-se da suscetibilidade de o objeto da análise sofrer alguma ação adversa, a fraqueza do bem crítico a ser protegido, e ocorre sempre em situações estabelecidas no contexto interno do estudo. Isto é, a vulnerabilidade é a percepção que se faz diante da ameaça, dos pontos fracos que compõem o contexto interno da análise. Por esse motivo, trata-se de uma variável com alta possibilidade de redução por meio de medidas preventivas (ANDRADE, 2017).

Ameaças, por sua vez, são ações naturais e humanas, intencionais ou não (acidentes), que colocam em risco o bem a ser protegido. Referem-se notadamente a situações que não estão sob o controle do problema de decisão (contexto externo), mas que possuem influência para causar danos ou gerar crises. Por essa razão, geralmente não são variáveis controláveis. No entanto, em certos casos, podem ser neutralizadas, isoladas ou, ainda, controladas por meio de ações específicas (AVEN, 2017).

Assim, o cálculo dos riscos da metodologia ARP consiste na compreensão da probabilidade de um evento indesejado ocorrer, independentemente da magnitude de seus efeitos, dada a sua real capacidade de subsidiar o planejamento para a segurança pessoal adequada com foco no risco.

3. METODOLOGIA ANÁLISE DE RISCO DE PESSOA

Com o objetivo de apoiar a abordagem para a elaboração de uma análise de riscos de pessoa, apresenta-se a estrutura geral da metodologia, com suas etapas e processos estabelecidos (Fig. 3).

FIGURA 3 – METODOLOGIA ANÁLISE DE RISCO DE PESSOA

Fonte: Elaborado pelos autores, adaptado de Orange Book (2021).

3.1. Estudo do Contexto

O processo de análise deve iniciar-se pela etapa da contextualização, ou, como foi identificada na metodologia, pelo "Estudo do Contexto". Trata-se da oportunidade de os profissionais envolvidos no estudo elaborarem um diagnóstico que contenha detalhes relevantes para a proteção da pessoa. A análise deve considerar os ambientes interno e externo, na medida em que ambos sofrem influências, diretas ou indiretas, de diferentes atores e de distintas naturezas que podem comprometer a integridade física do indivíduo.

Por ambientes interno e externo consideram-se os espaços e lugares em que a pessoa, habitual ou ocasionalmente, frequenta. Como exemplo, citam-se os locais de residência, trabalho, lazer, práticas religiosas, acadêmicas, esportivas etc. Importa nessa etapa conhecer a sua rotina, as suas vulnerabilidades – tanto de natureza física ou virtual – e as potenciais ameaças para que seja possível estabelecer um diagnóstico com a máxima precisão possível. A insuficiência de dados e informações inviabiliza a aplicação de qualquer modelo de análise de riscos.

Ao analisar o contexto de alguém que alega necessidade de segurança, geralmente a ameaça já é conhecida, o que se constitui como um facilitador ao processo de elaboração da análise de risco. Nesse sentido, a despeito da possibilidade de a ameaça se apresentar de forma múltipla, não percebida, ou mesmo desconhecida, um levantamento criterioso deve ponderar toda e qualquer possibilidade que possa

originar uma ameaça ou se constituir em fonte de risco (ISO 31000, 2018), na medida em que não há risco se não houver ameaça.

Com efeito, ao avaliar o contexto externo, deve-se observar se há relações e compromissos contratuais que apresentem pendências, por exemplo; eventuais atribulações nas redes de relacionamentos pessoal e profissional; considerar a percepção do próprio ameaçado é igualmente necessário. Ou seja, a ideia é proporcionar o máximo de amplitude possível à análise a fim de identificar a(s) ameaça(s) e, também, as vulnerabilidades existentes no processo.

Tanto a "ameaça" como a "vulnerabilidade" são variáveis essenciais ao modelo proposto e serão abordadas em seções específicas. Todavia, durante a concepção do "Estudo do Contexto" já é possível estabelecer caminhos, elaborar abstrações e identificar circunstâncias que contribuirão para a construção e análise da etapa posterior da metodologia, uma vez que essa reflexão se constitui como insumo à identificação desses elementos.

Para auxiliar nessa tarefa, e sem prejuízo de análises e conclusões que derivam da experiência dos profissionais envolvidos, sugere-se a utilização de técnicas que possam subsidiar no processo de inventário das ameaças e vulnerabilidades. Há diversas técnicas disponíveis, como o *Brainstorming*, Entrevistas estruturada e semiestruturada, *Checklist*, matriz *SWOT*, entre outras. Trata-se de ferramentas de aplicação simples e com potencial de contribuição relevante. Algumas dessas técnicas citadas, além de outras, estão previstas na norma (ISO 31010, 2012).

A matriz *SWOT*[4], por exemplo, é uma técnica utilizada para fazer análise de cenário (ou ambiente), em que um grupo de especialistas que conhecem o assunto representam graficamente os aspectos que consideram favoráveis (força e oportunidade) e desfavoráveis (fraquezas e ameaças). Ao proporcionar visão ampla dos ambientes interno e externo, a matriz permite ao time de analistas discernir melhor acerca do contexto analisado e, consequentemente, identificar ameaças e vulnerabilidades - elementos essenciais ao propósito da metodologia apresentada (SAMMUT-BONNICI; GALEA, 2014). A técnica é sugerida como facilitadora no processo e não deve ser utilizada como único recurso disponível.

Dessa forma, o "Estudo do Contexto" visa a proporcionar conhecimento geral do estudo de risco que será elaborado e delinear os aspectos relacionados com a segurança da autoridade. Objetivamente, esta etapa deverá conter: i) o escopo a ser explorado pelos analistas; ii) a descrição dos aspectos relacionados às atitudes, comportamentos e hábitos que sejam relevantes ao processo de identificação das vulnerabilidades; e iii) a apresentação minuciosamente a ameaça, caracterizando-a com o máximo de detalhes possíveis.

Ao cumprir esses pré-requisitos, o "Estudo de Contexto" proporcionará subsídios para a consecução das etapas subsequentes da metodologia, inclusive a identificação de medidas e procedimentos que possam ser adotados no sentido de propiciar mais segurança à pessoa que terá sua segurança avaliada.

Fatores humanos e culturais influenciam significativamente nos elementos de risco considerados na análise. Por mais que se conheça detalhadamente o comportamento de uma pessoa e represente-o por meio de texto ou fluxograma, o que permitiria identificar as principais vulnerabilidades, ainda assim, seria impossível estabelecer um modelo que proporcione proteção total.

4 *SWOT* é o acrônimo, em inglês, das palavras: Strenghts (Forças), Weaknesses (Fraquezas), Opportunities (Oportunidades) e Threats (Ameaças). No Brasil, ela também é conhecida por FOFA, acrônimo para Força, Oportunidade, Fraqueza e Ameaça (SAMMUT-BONNICI; GALEA, 2014).

3.2. Identificação dos Elementos do Risco

Conforme exposto, quando se analisam riscos relacionados à segurança de pessoas, são observados, invariavelmente, os riscos que comprometem a integridade física de um indivíduo e que podem resultar em lesões em diferentes níveis ou até mesmo a morte. Isto é, outros riscos podem ser indicados, como danos à imagem, vazamento de informações sensíveis etc. Todavia, o objetivo fundamental da metodologia é a integridade física da pessoa em análise.

Nesse contexto e de acordo com o foco apresentado, as consequências sobre a vida, em qualquer medida, são inegociáveis, motivo pelo qual a metodologia proposta centra-se na análise dos elementos do risco que estão relacionados com a probabilidade de um evento indesejado ocorrer, quais sejam, a ameaça e a vulnerabilidade.

Como reflexo, o processo de construção da metodologia ARP consiste na identificação, análise e avaliação das ameaças e vulnerabilidades observadas a partir do diagnóstico elaborado pela equipe de especialistas envolvida no processo.

3.2.1 Ameaça

A metodologia ARP postula que o risco será conhecido por meio da soma da ameaça e da vulnerabilidade. Nesse sentido, faz-se necessário identificar e valorar essas duas variáveis para que seja possível conhecer o grau de risco.

Independentemente do objetivo, e por mais que sejam identificadas inúmeras vulnerabilidades no contexto analisado, se não há ameaça que possa explorá-las, já que o sujeito da ação não existe, então eventuais e potenciais riscos não serão analisados. Ou seja, não há risco caso a ameaça não esteja endereçada.

A ameaça pode ser explicada em duas perspectivas de diferentes naturezas. Em uma perspectiva, a ameaça se define como um ato hostil praticado por ação humana contra uma determinada pessoa (RENN, 1992). Trata-se de uma ameaça ostensiva, deliberada, em que o ameaçador admite e anuncia seu propósito de realizar ato que resulte em dano a outrem.

Em outra perspectiva, a ameaça pode ser compreendida como um evento - ou um cenário - capaz de ocasionar prejuízo a uma pessoa. Comumente, essa ameaça se configura de forma velada, involuntária e até imperceptível (RENN, 1992). Diante disso, por ser circunstancial, a ameaça deriva de uma situação de perigo assumida pelo indivíduo, como um comportamento negligente ao dirigir em alta velocidade em uma pista molhada, por exemplo. Nesse caso, a exposição ao perigo pode aumentar a probabilidade de que outras ameaças integrem a análise, como outros veículos, pedestres, pista escorregadia, entre outras.

Ameaças de qualquer natureza são difíceis de controlar. Caso origine-se de um indivíduo, então é recomendado identificar, qualificar e valorar essa ameaça para que seja possível adotar medidas protetivas que representem redução, ou até mesmo a completa neutralização, da capacidade de ação do ameaçador.

Quanto à situação de perigo assumida por uma pessoa, expondo-a a ameaças e riscos involuntários, sugere-se o seu mapeamento e consequente ajuste de comportamento ou atitude que as originam, por meio de protocolos de atuação, relacionados às vulnerabilidades – e não à ameaça.

Dessa forma, os perigos que surgem do contexto interno, ou seja, que derivam de negligência, imprudência ou imperícia, por exemplo, devem ser analisados de forma detida, porque podem representar vulnerabilidades não verificadas quando da análise sob a perspectiva da ameaça externa. Essas fragilidades podem ser vistas como oportunidades para que potenciais agressores externos pratiquem seu intento.

Para classificar a ameaça, a metodologia ARP sugere uma estrutura a partir de quatro variáveis: potencial, motivação, influência e histórico. Esses critérios possuem pesos diferentes, que devem ser definidos em função da relevância de cada um deles em um contexto de ameaça.

As variáveis: potencial, motivação e influência são identificadas pelo auxílio de uma escala com cinco graus, que compreende o intervalo entre o menor grau (muito baixo) até o maior grau (muito alto). Os graus são associados a valores definidos por meio de acordo semântico. Trata-se de uma escala de autorrelato, em que o especialista responde às questões propostas na escala, sem influência externa. Nesse caso, a escala proposta é a de Likert[5], em que o analista manifesta seu grau de adesão às assertivas da escala ao indicar, dentre os cinco níveis propostos, o nível de concordância ou discordância em função da ameaça avaliada.

A variável: histórico também será definida pelo auxílio de uma escala com cinco graus, porém o menor grau será identificado como "inexistente" e não "muito baixo", como é nas demais variáveis. O maior grau é idêntico às outras variáveis, ou seja, "muito alto". O fato de não haver histórico não significa que não possa vir a ocorrer. Nesse sentido, alerta-se que o "gerente de risco erra ao olhar no retrovisor para enxergar o futuro" Taleb e Spitznagel (2014, p. 3). Os autores lembram que não havia precedentes para eventos como a 1ª Guerra Mundial e os ataques de 11 de setembro de 2001. Daí deriva-se o motivo pelo qual, nesta metodologia, o histórico possui um peso de 10% na valoração da ameaça, na medida em que os demais elementos irão ajustar uma eventual distorção.

A variável "Potencial" se refere à capacidade - técnica, logística e financeira - do autor da ameaça. Na metodologia aqui proposta, a variável corresponde a 40% do peso total na sua avaliação, mas pode ser adaptada de acordo com a especificidade da análise (Quadro 1).

5 A escala de Likert foi desenvolvida pelo cientista Rensis Likert. Apresenta-se como uma tabela de classificação em que o respondente é convidado a emitir o seu grau de concordância ao indicar, dentre as frases que representam os níveis da escala, a que melhor traduz sua opinião (JOSHI *et al*., 2015).

QUADRO 1: ESCALA DE AVALIAÇÃO DO POTENCIAL DA AMEAÇA

POTENCIAL (peso: 40%)		
Grau	**Valor**	**Descrição**
Muito alto	5	O autor da ameaça possui plena capacidade técnica, logística e financeira para concretizar a ação adversa
Alto	4	O autor da ameaça possui alta capacidade técnica, logística e financeira para concretizar a ação adversa
Médio	3	O autor da ameaça possui média capacidade técnica, logística e financeira para concretizar a ação adversa
Baixo	2	O autor da ameaça possui baixa capacidade técnica, logística e financeira para concretizar a ação adversa
Muito baixo	1	O autor da ameaça possui insignificante capacidade técnica, logística e financeira para concretizar a ação adversa

Fonte: Elaborado pelos autores (2021).

A "Motivação", por sua vez, consiste na compreensão e avaliação do pretexto que induziu o ameaçador a proferir a ameaça. Geralmente está associada a questões ideológicas ou refere-se à retaliação em função de ação pretérita sob responsabilidade da pessoa ameaçada. Corresponde a 40% do peso total na avaliação, assim como a variável "Potencial".

QUADRO 2: ESCALA DE AVALIAÇÃO DA MOTIVAÇÃO DA AMEAÇA

MOTIVAÇÃO (peso: 40%)		
Grau	**Valor**	**Descrição**
Muito alto	5	Há elementos, ou grupos, plenamente motivados, criminal ou ideologicamente, direta ou indiretamente.
Alto	4	Há elementos, ou grupos, altamente motivados, criminal ou ideologicamente, direta ou indiretamente.
Médio	3	Há elementos, ou grupos, relativamente motivados, criminal ou ideologicamente, direta ou indiretamente.
Baixo	2	Há elementos, ou grupos, pouco motivados, criminal ou ideologicamente, direta ou indiretamente.
Muito baixo	1	Há elementos, ou grupos, sem motivação, criminal ou ideologicamente, direta ou indiretamente.

Fonte: Elaborado pelos autores (2021).

Na variável "Influência" verifica-se o poder de decisão do ameaçador. Se ele pertence a uma organização criminosa, por exemplo, avalia-se sua autoridade e importância na hierarquia do grupo. A citação a uma organização criminosa serve como referência, mas, mesmo se não houver indícios de pertencimento a uma organização criminosa, procura-se avaliar a capacidade de intervir ou interceder junto a outros grupos, no sentido de viabilizar a concretização da ação adversa contida na ameaça. Estabeleceu-se em 10% do peso total na avaliação da ameaça e é representada de acordo com o Quadro 3:

QUADRO 3: ESCALA DE AVALIAÇÃO DA INFLUÊNCIA DA AMEAÇA

INFLUÊNCIA (peso: 10%)		
Grau	**Valor**	**Descrição**
Muito alto	5	O autor da ameaça é chefe de organização criminosa e/ou possui pleno poder de decisão
Alto	4	O autor da ameaça é integrante de destaque em organização criminosa e/ou possui considerável poder de decisão.
Médio	3	O autor da ameaça é integrante comum de organização criminosa e/ou possui relativo poder de decisão.
Baixo	2	O autor da ameaça não pertence a organização criminosa e/ou possui baixo poder de decisão.
Muito baixo	1	O autor da ameaça não pertence a organização criminosa e/ou não possui qualquer poder de decisão.

Fonte: Elaborado pelos autores (2021).

Última variável a ser considerada na valoração da ameaça, o "Histórico" sugere a análise com base em registros pretéritos de ameaças concretizadas. Normalmente é difícil associar o cometimento de crimes de homicídio aos autores da ameaça, até pela dificuldade de elucidação de crimes dessa natureza, de indicação da autoria e materialidade.

Entretanto, a despeito desse contratempo, é possível que os analistas envolvidos na avaliação tenham acesso a informações seguras e confiáveis que permitam algum nível de associação da ameaça concreta a eventos que culminaram em homicídio ou tentativa de homicídio. Nesse caso, o grau de certeza do analista com relação às fontes utilizadas deve ser considerado. A variável "Histórico" corresponde a 10% do peso total na avaliação da ameaça e será avaliada por meio da escala, conforme contido no Quadro 4:

QUADRO 4: ESCALA DE AVALIAÇÃO DO HISTÓRICO DA AMEAÇA

HISTÓRICO (peso: 10%)		
Grau	**Valor**	**Descrição**
Muito alto	5	Com base no histórico, muito provavelmente a ameaça se concretizará.
Alto	4	Com base no histórico, provavelmente a ameaça se concretizará.
Médio	3	Com base no histórico, possivelmente a ameaça se concretizará.
Baixo	2	Com base no histórico, é improvável que a ameaça se concretize.
Inexistente	1	Não há histórico.

Fonte: Elaborado pelos autores (2021).

Para realizar a avaliação e valoração da ameaça com base nas quatro variáveis apresentadas, sugere-se o mínimo de três especialistas. O objetivo é promover mais equilíbrio ao minimizar a possibilidade de avaliações extremas, já que a média entre distintas perspectivas são traduzidas em um ponto comum. A título de exemplo, e considerando a avaliação hipotética das quatro variáveis por três especialistas, tem-se um resultado semelhante ao demonstrado no Quadro 5:

QUADRO 5: DEMONSTRATIVO DO CÁLCULO DA AMEAÇA

AMEAÇA						
Variáveis	**Esp 1**	**Esp 2**	**Esp 3**	**Média**	**Peso %**	**Nota**
Potencial	2	3	2	2,3	40%	0,9
Motivação	5	3	2	3,3	40%	1,3
Influência	3	2	3	2,7	10%	0,3
Histórico	2	2	2	2,0	10%	0,2
Totais	**12**	**10**	**9**	**10,3**	**100%**	**2,7**

Fonte: Elaborado pelos autores (2021).

Como se pode observar no Quadro 5, após avaliação das variáveis por cada especialista, apura-se a média das notas atribuídas. Para calcular a média, somam-se as notas de cada votante e divide-se o resultado pelo número de especialistas participantes.

A nota de cada variável será o produto extraído da média multiplicado pelo peso percentual de cada variável. Dessa forma, o valor será a soma das notas, que no exemplo acima é igual a 2,7 de um total máximo de 5, o que representa 54%. Finalmente, após a avaliação da ameaça, submete-se o valor apurado à escala de classificação, que vai indicar o nível da ameaça, conforme Quadro 6:

QUADRO 6: DEMONSTRATIVO DO CÁLCULO DA AMEAÇA

Nível da Ameaça	Valor	%
Severa	4 - 5	80% - 100%
Significante	3 - 3,99	60% - 79,9%
Moderada	2 - 2,99	40% - 59,9%
Pequena	1,5 - 1,99	30% - 39,9%
Insignificante	1,0 - 1,49	20% - 29,9%

Fonte: Elaborado pelos autores (2021).

De acordo com a escala sugerida, a ameaça será classificada com o nível "moderada", já que tem valor 2,7, representado pelo intervalo percentual entre 40% e 59,9%. Ressalte-se que, se houver mais de uma ameaça identificada, o processo de análise e valoração deverá ser conduzido individualmente.

Dessa forma, para se obter o nível de risco, além de valorar a ameaça, faz-se necessário conhecer as vulnerabilidades, próxima etapa do processo.

3.2.2 Vulnerabilidades

Identificam-se as vulnerabilidades a partir da compreensão das atitudes e comportamentos adotados, direta ou indiretamente, pela pessoa a ser protegida. A forma indireta se refere às atitudes e comportamentos de pessoas próximas ao dignitário que terá sua proteção analisada. Vulnerabilidades são características intrínsecas de algo que resulta em suscetibilidade a uma fonte de risco que pode levar a um evento com uma consequência (ABNT ISO 73, 2009).

No caso específico, vulnerabilidade pode ser compreendida como a identificação de fragilidades que podem ser exploradas pelas ameaças para a perpetração de ato hostil contra uma pessoa. Na trajetória do risco, as vulnerabilidades podem ser comparadas à porta que dá acesso à ameaça. Mesmo que todas as supostas vulnerabilidades sejam identificadas e as respectivas medidas de tratamento implementadas, ainda assim, sempre haverá risco. O fator humano é uma variável imprevisível, suscetível a influências imperceptíveis e de distintas naturezas, o que permite afirmar, como corolário, que não há segurança completamente eficiente.

Com esse entendimento, e para mitigar os impactos do imponderável que emerge da natureza humana, percebe-se a importância de planejar as categorias vulneráveis que serão avaliadas para mapear as fragilidades apresentadas pela pessoa a ser protegida, de forma que os riscos sejam compreendidos e geridos.

Nessa perspectiva, a ARP prevê a elaboração de uma lista de vulnerabilidades relacionadas ao contexto da pessoa que está sob perigo ou ameaça. O mapeamento delas deve considerar distintos aspectos do cotidiano do indivíduo, da forma mais analítica possível, e desde que haja alguma relação com potenciais riscos. Detalhes da vida pessoal e profissional devem ser compreendidos e traduzidos em "itens de vulnerabilidade", que é a forma como a metodologia convencionou chamar.

A lista de vulnerabilidades deve ser organizada em categorias e subcategorias vulneráveis e será analisada individualmente pelos analistas que desenvolvem o trabalho. A relação de vulnerabilidades deve ser adaptada às diferentes circunstâncias que se relacionam à rotina do dignitário e deve abranger tanto o âmbito pessoal e profissional quanto os meios físico e virtual.

Cada detalhe é importante para a análise: se a pessoa mora em apartamento ou casa; se o condomínio é aberto ou fechado; se há porteiro, garagem privativa, segurança 24 horas; ou se a região é conhecida como violenta. Também se o indivíduo costuma visitar bares, clubes e eventos sociais de forma regular ou inopinada. O mesmo exercício se aplica ao local de trabalho.

A compreensão da rotina da autoridade permitirá a identificação das vulnerabilidades que podem ser exploradas pelas ameaças para a concretização de ato hostil. Com efeito, percebe-se que se trata de um elemento de natureza personalíssima e, portanto, não há um modelo de categorização de vulnerabilidades que possa contemplar todo o escopo, de modo exaustivo. Ele deve ser construído em função do contexto estabelecido.

Para ilustrar o que foi sugerido, o Quadro 7 apresenta um exemplo com cinco categorias vulneráveis e suas respectivas subcategorias. Salienta-se que não há limite definido de categorias e subcategorias vulneráveis, já que o processo é individual, adaptado à realidade factual.

QUADRO 7: DEMONSTRATIVO DE CATEGORIAS E SUBCATEGORIAS VULNERÁVEIS

CATEGORIAS E SUBCATEGORIAS VULNERÁVEIS
1. Áreas e Instalações
1.1 Sistema de Barreira Física
1.2 Sistema de Controle de Acesso
1.3 Sistema de Monitoramento
2. Recursos Humanos
2.1 Vigilância
2.2 Funcionários
2.3 Prestadores de Serviços
3. Administração do Material Sensível
3.1 Crachá
3.2 Chaves
4. Exposição
4.1 Exposição Virtual
4.2 Exposição Física
5. Controles
5.1 Procedimentos e Protocolos

Fonte: Elaborado pelos autores (2021).

O exemplo acima apresenta cinco categorias vulneráveis: áreas e instalações, recursos humanos, administração do material sensível, exposição e controles, e as suas respectivas subcategorias. Conforme mencionado, não há um modelo que atenda às peculiaridades de cada pessoa que necessita de proteção.

Assim, no modelo ilustrativo, percebe-se que a categoria Controles possui apenas uma subcategoria: Procedimentos e Protocolos. Possivelmente, em uma situação real, a equipe de analistas pode identificar a necessidade de separar o item vulnerável "Procedimentos e Protocolos" em dois itens distintos: "Procedimentos" e "Protocolos", ou inserir outras subcategorias para poder analisar características específicas, ou até mesmo excluir a categoria Controles. O importante é que a lista contemple todo o contexto de vulnerabilidades em que a autoridade esteja inserida.

Uma vez definidas as categorias e consequentes subcategorias de vulnerabilidades, devem-se identificar os itens de vulnerabilidades que compõem cada subcategoria, de forma analítica. Cada item de vulnerabilidade inserido corresponde a uma variável que pode comprometer a segurança. Da mesma forma, cada subcategoria será composta de quantos itens de vulnerabilidade forem necessários para analisar esse elemento do risco.

Para ilustrar essa etapa da metodologia, o Quadro 8 apresenta duas categorias; cada uma contém duas subcategorias; e, por fim, para cada subcategoria foram identificadas duas vulnerabilidades.

QUADRO 8: LISTA DE VULNERABILIDADE

VULNERABILIDADES	
1. Categoria	Áreas e Instalações
1.1 Subcategoria	Sistema de Barreira Física
Portaria 24 horas	
Perímetro monitorado por CFTV	
1.2 Subcategoria	Sistema de Controle de Acesso
Triagem e cadastramento de pessoas e veículos	
Acessos possuem cancelas ou portões	
2. Categoria	Exposição
2.1 Subcategoria	Exposição Virtual
Redes sociais própria	
Locais visitados (*check in virtual*)	
2.2 Subcategoria	Exposição Física
Itinerário ordinário	
Alternância de rota	

Fonte: Elaborado pelos autores (2021).

Uma vez identificados os itens de vulnerabilidade relacionados à segurança da autoridade, e organizados nas subcategorias e categorias vulneráveis correspondentes, os especialistas que conduzem o processo devem avaliar cada item vulnerável.

Essa valoração consiste na atribuição de notas para os itens de vulnerabilidade identificados, representado por um vocábulo ou uma frase que conduz o avaliador a interpretar uma situação que pode comprometer a segurança da autoridade. À interpretação é atribuída uma nota constante de escala, previamente elaborada, com descrições verbais que estabelecem patamares em acordos semânticos:

QUADRO 9: ESCALA DE AVALIAÇÃO DE VULNERABILIDADES

Nota	Descrição
0	O controle é desnecessário
0,5	O controle é adequado e eficiente
2	O controle necessita de pequenos ajustes para melhor adequação e eficiência
3,5	O controle necessita de significativos ajustes para melhor adequação e eficiência
5	Não existe controle ou o controle utilizado é inadequado e/ou ineficiente

Fonte: Elaborado pelos autores (2021).

Avalia-se o item de vulnerabilidade submetendo-o à escala sugerida. Ao analisar, por exemplo, o item vulnerável identificado como "Portaria 24h", faz-se o confronto entre a situação real da autoridade e a situação ideal, para um padrão de segurança aceitável, na interpretação de cada especialista que participa do processo de avaliação de riscos.

A título de exemplo, se a autoridade mora em um prédio em que a portaria só funciona no horário comercial e um dos especialistas entende que deveria haver portaria 24h, então, de acordo com a

escala sugerida, esse especialista poderia atribuir nota 3,5 (controle necessita de ajustes significativos). Por outro lado, se outro analista que participa do processo entende que a portaria funcionar durante o horário comercial atende às questões de segurança, o que não o exporia a riscos, então esse analista poderia atribuir nota 0,5 (controle adequado e eficiente).

Portanto, recomenda-se que os itens de vulnerabilidades sejam analisados por três especialistas, no mínimo, e que todos que participam do processo conheçam o contexto interno e externo, para poder avaliar com mais fidedignidade. É essencial que os profissionais envolvidos na avaliação tenham acesso às mesmas informações coletadas sobre o dignitário que está com a segurança sob análise, bem como tenham participado dos levantamentos no local relevantes para a elaboração do estudo. Essas são premissas que traduzem uma avaliação mais próxima da realidade.

Após a análise individual dos votantes, os itens vulneráveis devem receber uma valoração, que será a média da somatória das notas dos especialistas: Item Vulnerável = ∑ (especialista 1; especialista 2; especialista 3) /3.

Esse procedimento deve ser repetido individualmente para todos os itens de vulnerabilidade que forem identificados no processo de análise. Dessa forma, obtém-se o índice de vulnerabilidade de cada subcategoria. Uma vez apurado o seu índice, obtém-se, também, o valor de vulnerabilidade das respectivas categorias vulneráveis.

Os Quadros 10 e 11, a seguir apresentados, indicam a forma de cálculo da vulnerabilidade utilizando-se apenas duas categorias vulneráveis: "Áreas e instalações" e "Exposição". Salienta-se que é preciso considerar todas as categorias para o cálculo geral da vulnerabilidade do sistema.

QUADRO 10: AVALIAÇÃO DAS VULNERABILIDADES DA CATEGORIA: ÁREAS E INSTALAÇÕES

1. CATEGORIA	**ÁREAS E INSTALAÇÕES**			
1.1 Subcategoria	Sistema de Barreira Física	Avaliação dos Especialistas		
Descrição da Vulnerabilidade		Esp 1	Esp 2	Esp 3	Média
Portaria 24h		0,5	2	3,5	2
Perímetro monitorado por CFTV		2	2	0,5	1,5
Total da subcategoria: Sistema de Barreira Física		2,5	4	4	3,5
Vulnerabilidade da subcategoria: Sistema de Barreira Física					1,75
1.2 Subcategoria	Sistema de Controle de Acesso	Avaliação dos Especialistas		
Descrição da Vulnerabilidade		Esp 1	Esp 2	Esp 3	Média
Triagem e cadastramento de pessoas e veículos		0,5	0,5	2	1
Acessos possuem cancelas ou portões		2	2	2	2
Total da subcategoria: Sistema de Controle de Acesso		2,5	2,5	4	3
Vulnerabilidade da subcategoria: Sistema de Controle de Acesso					1,5
Total da categoria: Áreas e Instalações		5	6,5	8	6,5
VULNERABILIDADE CATEGORIA: ÁREAS E INSTALAÇÕES					**1,63**

Fonte: Elaborado pelos autores (2021).

A vulnerabilidade da categoria "Áreas e Instalações" é igual a 1,63. Esse valor foi obtido a partir da soma das duas subcategorias: Sistema de Barreira Física (1,75) e Sistema de Controle de Acesso (1,5),

e o resultado dividido por dois, total de subcategorias utilizadas. O valor da vulnerabilidade da subcategoria segue a mesma lógica. Somam-se as médias dos itens de vulnerabilidade e o resultado é dividido pelo total de itens considerados na soma. No caso da subcategoria Sistema de Controle de Acesso, o total 1,5 é resultado do total da subcategoria (3) dividido pela quantidade de itens somados (2).

Da mesma forma, a Quadro 11 traz o cálculo da vulnerabilidade da categoria "Exposição":

QUADRO 11: AVALIAÇÃO DAS VULNERABILIDADES DA CATEGORIA EXPOSIÇÃO

2. CATEGORIA	**EXPOSIÇÃO**			
2.1 Subcategoria	Exposição Virtual	Avaliação dos Especialistas		
Descrição da Vulnerabilidade		Esp 1	Esp 2	Esp 3	Média
Redes sociais própria		3,5	5	3,5	4
Locais visitados (check in)		5	5	5	5
Total da subcategoria: Exposição Virtual		8,5	10	8,5	9
Vulnerabilidade da subcategoria: Exposição Virtual					4,5
2.2 Subcategoria	Exposição Física	Avaliação dos Especialistas		
Descrição da Vulnerabilidade		Esp 1	Esp 2	Esp 3	Média
Itinerário ordinário		3,5	3,5	3,5	3,5
Alternância de rota		3,5	2	0,5	2
Total da subcategoria: Exposição Física		7	5,5	4	5,5
Vulnerabilidade da subcategoria: Exposição Física					2,75
Total da categoria: Exposição		15,5	15,5	12,5	14,5
VULNERABILIDADE DA CATEGORIA: EXPOSIÇÃO					**3,63**

Fonte: Elaborado pelos autores (2021).

Caso o especialista atribua nota zero a um item vulnerável inserido na avaliação, ou seja, considerar que "o controle é desnecessário", então esse item vulnerável deverá ser desconsiderado no cômputo total.

Concluída a valoração dos itens de vulnerabilidade e já com os somatórios das subcategorias e categorias realizados, é necessário apurar a vulnerabilidade total, traduzida pela média das categorias.

Como reflexo, a metodologia ARP propõe que o Fator de Vulnerabilidade do sistema é conhecido a partir do resultado da soma das notas das categorias vulneráveis dividido pela quantidade de categorias consideradas no levantamento. No exemplo apresentado, deve-se somar a vulnerabilidade da categoria "Áreas e instalações" (1,63) com a categoria "Exposição" (3,63). O resultado deve ser dividido por 2, que é a quantidade de categorias consideradas no modelo. Ao realizar essa operação, chega-se ao "Fator de Vulnerabilidade" do sistema, que é 2,63.

O estudo das vulnerabilidades de uma pessoa quanto à sua segurança permite analogia à Teoria do Queijo Suíço[6], ao analisá-las em camadas de proteção e as suas subjacentes fragilidades. Da mesma forma, ao considerar o processo de segurança de uma pessoa como uma sucessão de fatias de queijos suíços, uma trajetória de falhas na segurança da autoridade pode resultar no alinhamento dos buracos do queijo, ocasionando um evento que pode significar comprometimento da segurança.

6 Teoria do Queijo Suíço é um modelo proposto por James Reason, professor de psicologia da Universidade de Manchester, no Reino Unido (REASON, 1990).

Como recurso didático, para uma melhor visualização gerencial, sugere-se demonstrar esses cálculos de forma consolidada, conforme o Quadro 12, abaixo.

QUADRO 12: ANÁLISE DAS VULNERABILIDADES

CATEGORIAS VULNERÁVEIS		Nota das Categoriais e Subcategorias Vulneráveis	Fator de Vulnerabilidade do Sistema Avaliado
1. Áreas e Instalações		1,63	2,63
Subcategorias	1.1 Sistema de Barreira Física	1,75	
	1.2 Sistema de Controle de Acesso	1,50	
2. Exposição		3,63	
Subcategorias	2.1 Exposição Virtual	4,50	
	2.2 Exposição Física	2,75	

Fonte: Elaborado pelos autores (2021).

Este processo facilita a gestão das vulnerabilidades ao apresentá-las de forma organizada e consolidada. Com efeito, as subcategorias e categorias vulneráveis com suas respectivas notas fornecem à equipe uma análise gerencial das vulnerabilidades, ao identificar as subcategorias que apresentam notas mais elevadas.

Uma vez conhecido o fator de vulnerabilidade total do contexto estudado, é necessário analisar o resultado com base na escala de classificação, que vai indicar o grau de vulnerabilidade:

QUADRO 13: ESCALA DE VULNERABILIDADE

Escala de Vulnerabilidade	
Nível de Vulnerabilidade	**Valor**
A vulnerabilidade analisada é muito alta	4 – 5
A vulnerabilidade analisada é alta	3 – 3,9
A vulnerabilidade analisada é média	2 – 2,9
A vulnerabilidade analisada é baixa	1 – 1,9
A vulnerabilidade analisada é muito baixa	0,5 – 0,9

Fonte: Elaborado pelos autores (2021).

De acordo com a escala, o nível de vulnerabilidade do contexto analisado será médio, uma vez que o fator de vulnerabilidade encontrado foi igual a 2,63 (Quadro 12), que se encaixa no nível que compreende o intervalo entre 2 e 2,9.

3.3 Estimativa do Risco

Após identificar, analisar e valorar os elementos do risco ameaça e vulnerabilidade, a próxima etapa consiste em estimar o seu nível. Este processo é realizado utilizando-se uma matriz, representada em forma de gráfico, que identifica a convergência entre a vulnerabilidade (eixo X) e a ameaça (eixo Y). O produto dessa dupla entrada indicará o grau de risco da pessoa que está com a segurança sob análise, em termos de probabilidade.

Uma vez que as escalas de ameaça e vulnerabilidade possuem cinco níveis cada um, optou-se pela matriz de risco com 25 quadrantes, distribuídos em cinco classificações de risco: muito baixo, baixo, moderado, alto e extremo, conforme Figura 4.

FIGURA 4: MATRIZ DE RISCO ANÁLISE DE RISCO DE PESSOA

Matriz de Risco		Vulnerabilidade				
		Muito Baixa	Baixa	Média	Alta	Muito Alta
Ameaça	Insignificante	MB	MB	BA	BA	MO
	Pequena	MB	BA	BA	MO	MO
	Moderada	BA	BA	MO	MO	AL
	Significante	BA	MO	MO	AL	EX
	Severa	MO	MO	AL	EX	EX

Fonte: Elaborado pelos autores (2021).

Ao realizar a dupla entrada na matriz, ou seja, combinar os níveis encontrados para as variáveis ameaça e vulnerabilidade, encontra-se o respectivo grau de risco. Esse procedimento deve ser elaborado de acordo com a quantidade de ameaças identificadas, isto é, para cada ameaça faz-se necessária uma análise específica. No exemplo citado tem-se, respectivamente, "Moderada" e "Média", o que significa que o risco é "Moderado".

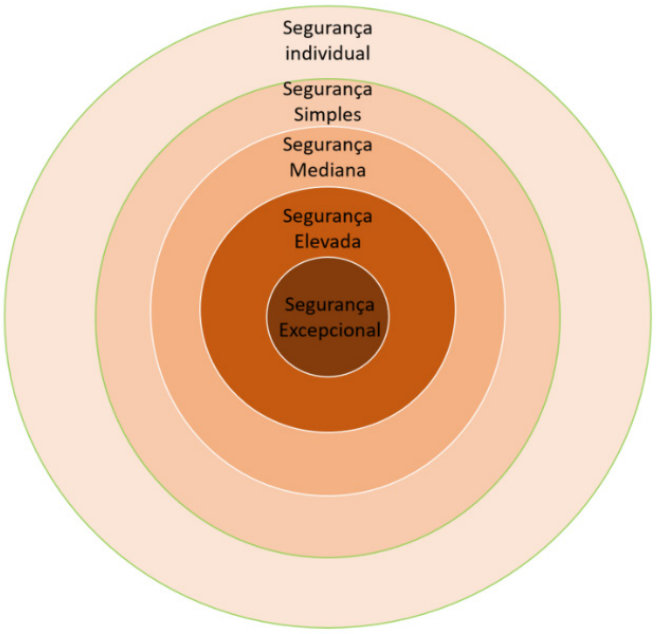
3.4 Medidas de Tratamento Requeridas

Por meio da compreensão dos elementos do risco, é possível sugerir ações mais eficazes para o seu tratamento, voltadas para auxiliar a condução de resultados objetivos que impliquem na redução da probabilidade de concretização de um evento indesejado ocorrer. Não obstante, a Análise de Riscos de Pessoa tem a capacidade de assessorar tanto com relação à priorização de tratamento como na vinculação de procedimentos em função do grau de risco identificado.

Tal qual como ocorre no caso da identificação de categorias vulneráveis, as recomendações de tratamento do risco irão depender de fatores próprios, tais como a capacidade financeira da pessoa, em se tratando de segurança privada, ou recursos institucionais, caso relacione-se a autoridades ou dignitários. Portanto, a disposição de um nível de proteção deve ser dimensionada para fazer frente aos riscos que recaem contra uma pessoa em específico.

Assim, para que haja uma análise bem estruturada, o modelo de detalhamento dos procedimentos de segurança dependerá das possibilidades do sistema em análise. Como sugestão, recomenda-se a utilização de processos de proteção em função dos graus de risco identificados, traduzidos por meio de círculos concêntricos. Dessa forma, serão necessários tantos círculos concêntricos quanto forem os procedimentos diferenciados de proteção, como, por exemplo:

FIGURA 5: PROCEDIMENTOS DE SEGURANÇA



Fonte: Elaborado pelos autores (2021).

O objetivo desse procedimento é estabelecer um equilíbrio entre a forma de atuação da equipe de proteção em função do risco identificado, ao fornecer adequabilidade no emprego de recursos às suas ações. A Figura 5 sugere cinco medidas, sem, contudo, especificar quais são, haja vista a impossibilidade de se retratar a capacidade protetiva de distintas análises.

4. CONSIDERAÇÕES FINAIS

Um planejamento de segurança deve ser entendido como a formulação de um conjunto de medidas – em sua maioria, preventivas – que visam a proteger a pessoa de potenciais ameaças. Não obstante, além da possiblidade de melhor identificar as vulnerabilidades de um determinado segurado – e sugerir o subjacente tratamento -, a ARP permite assessorar quanto à adequabilidade do nível de controle de que uma pessoa pode dispor em função do risco.

Dessa forma, para uma proteção adequada, entende-se que a análise de risco é o alicerce básico para o planejamento da segurança pessoal, ao possibilitar compreender os elementos que são influenciados e podem influenciar na concretude de um dado risco.

Trata-se, sobretudo, de uma ferramenta que auxilia a tomada de decisão de natureza preventiva, pelo que processa os dados de forma analítica e fornece conhecimento para abordagem sistemática e disciplinada para a avaliação e a melhoria da eficácia dos processos de proteção.

REFERÊNCIAS

ANDRADE, F. S. **Análise de riscos estratégicos:** proposição de uma metodologia com foco nos valores organizacionais a partir do contexto da segurança pública. 2019. 104 f. Dissertação (Mestrado em Engenharia da Produção) – Universidade Federal de Pernambuco, Recife, 2019. Disponível em: https://repositorio.ufpe.br/handle/123456789/34550. Acesso em: 3 jun. 2021.

ANDRADE, F. S. ROCKEMBACH, Silvio Jacob. Metodologia ARSO: Análise de Riscos em Segurança Orgânica. **Revista Mercopol. Edición Paraguay**.[*s. l.*], n. 11, v. 11, 2018. ISSN 2236-9236.

ANDRADE, F. S. Análise de Riscos e a Atividade de Inteligência. **Revista Brasileira de Ciências Policiais**, Brasília, v.8, n. 2, p. 91-116, 2017. DOI: https://doi.org/10.31412/rbcp.v8i2.462. Disponível em: https://periodicos.pf.gov.br/index.php/RBCP/article/view/462. Acesso em: 14 ago. 2021.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ISO GUIA 73**: gestão de riscos: vocabulário. Rio de Janeiro: ABNT, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ISO/IEC 31010**: gestão de riscos: técnicas de avaliação de riscos. Rio de Janeiro: ABNT, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 31000**: gestão de riscos: diretrizes. Rio de Janeiro: ABNT, 2018.

AVEN, T. Risk assessment and risk management: Review of recent advances on their foundation. **European Journal of Operational Research**. [*s. l.*], v. 253, p. 1-13, 16 ago. 2016. DOI: https://doi.org/10.1016/j.ejor.2015.12.023. Disponível em: https://www.sciencedirect.com/science/article/pii/S0377221715011479. Acesso em: 14 ago. 2021.

BRASIL. Ministério do Planejamento, Orçamento e Gestão e a Controladoria Geral da União. **Instrução Normativa Conjunta MPOG e CGU nº1, de 10 de maio de 2016**. Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal. Brasília, DF: Ministério do Planejamento, Orçamento e Gestão e a Controladoria Geral da União, 10 maio 2016. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/21519355/do1-2016-05-11-instrucao-normativa-conjunta-n-1-de-10-de-maio-de-2016-21519197. Acesso em: 14 ago. 2021.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY

COMISSION. **Enterprise Risk Management – Integrated Framework**. [*s. l.*]: COSO, 2004.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. **The 2013 COSO framework & SOX compliance:** one approach to an effective transition. [*s. l.*]: COSO, 2013.

COOKE, R. **Experts in uncertainty:** opinion and subjective probability in science. New York: Ed. Oxford University Press, 1991.

CRESWELL, J. W. **Research Design:** qualitative, quantitative, and mixed methods approaches. Nebraska: Ed. Sage, 2003.

FINE, W. T. Mathematical Evaluations for Controlling Hazards. **Journal of Safety Research**. [*s. l.*], v. 3, n. 4, p. 157-166, 8 mar. 1971.

INTERNATIONAL ORGANIZATION FOR STANDARTIZATION. Risk management - Principles and guidelines. **ISO 31000:2018**, Geneva, 2018.

JOSHI, A.; KALE, S.; CHANDEL, S.; Pal, D. K. Likert scale: Explored and explained. **British journal of applied science & technology**, [*s. l.*], v. 7, n. 4, p. 396-403, 2015.

KOVACICH, G.; HALIBOZEK, E. P. **Security metrics management**. New York: Elsevier Inc, 2006.

LANDOLL, D. **The security risk assessment handbook**. Auerbach Publications, New York, 2006. 490 p.

MANDARINI, M. A. **Segurança corporativa estratégica:** fundamentos. São Paulo: Manole, 2005. 350 p.

NORMAN, T. L. **Risk analysis and security countermeasure selection**. CRC Press, 2010. 484 p.

PORTELLA, P. R. A. **Gestão de Segurança: segurança privada, sistemas de produção, historia, metodologia e doutrina**. Rio de Janeiro: Editora Rio, 2004.

REASON, J. **Human error.** New York: Cambridge University Press, 1990. 320 p. Disponível em: https://www.cambridge.org/highereducation/books/human-error/281486994DE4704203A514F7B7D826C0#overview. Acesso em: 8 ago. 2021.

RENN, O. Concepts of risk: a classification. *In:* **Social theories of risk**. Westport, Conn, 1992. p. 53-79. DOI: http://dx.doi.org/10.18419/opus-7248. Disponível em: https://elib.uni-stuttgart.de/handle/11682/7265. Acesso em: 8 ago. 2021.

RODRÍGUEZ, J.; CONTRERAS, B. M. G. Operational Risk: applying the Mosler methodology in production sector in Mexico. **International Journal of Science and Research**, [*s. l.*], v. 3, n. 7, p. 451-454, 2014.

SAMMUT-BONNICI, T.; GALEA, D. SWOT analysis. In: Cooper CL, ed. Wiley **Encyclopedia of Management**, [*s. l.*], v. 12, p. 1-8, 2014. DOI 10.1002/9781118785317.weom120103. Disponível em: https://onlinelibrary.wiley.com/doi/10.1002/9781118785317.weom120103. Acesso em: 14 ago. 2021.

TALEB, N.; GOLDSTEIN, G.; SPITZNAGEL, M. **Seis erros que o executivo comete na gestão de riscos**. [*s. l.*]: Harvard Business Review, out. 2009. Disponível em: https://hbr.org/2009/10/the-six-mistakes-executives-make-in-risk-management?language=pt/. Acesso em: 22 maio 2021.

UNITED KINGDOM. **The Orange Book Management of Risk: principles and concepts**. London: HM Treasury, 2013.

WILLIAMS, R. **Keywords: a vocabulary of culture and society**. New York: Ed. Oxford University Press, 1985.