UFRRJ
INSTITUTO DE CIÊNCIAS SOCIAIS APLICADAS
PROGRAMA DE PÓS GRADUAÇÃO EM GESTÃO E ESTRATÉGIA
MESTRADO PROFISSIONAL EM GESTÃO E ESTRATÉGIA - MPGE

DISSERTAÇÃO

PROPOSIÇÃO, APLICAÇÃO E VALIDAÇÃO DE UM *FRAMEWORK* DE AVALIAÇÃO DE RISCOS, APLICADO AO COMPARTILHAMENTO DE SISTEMAS DE RADIOCOMUNICAÇÕES DE UM ÓRGÃO DE SEGURANÇA PÚBLICA

ALUISIO SARDINHA GARCIA

2020

UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
INSTITUTO DE CIÊNCIAS SOCIAIS APLICADAS
PROGRAMA DE PÓS-GRADUAÇÃO EM GESTÃO E ESTRATÉGIA
MESTRADO PROFISSIONAL EM GESTÃO E ESTRATÉGIA - MPGE

PROPOSIÇÃO, APLICAÇÃO E VALIDAÇÃO DE UM *FRAMEWORK* DE AVALIAÇÃO DE RISCOS, APLICADO AO COMPARTILHAMENTO DE SISTEMAS DE RADIOCOMUNICAÇÕES DE UM ÓRGÃO DE SEGURANÇA PÚBLICA

ALUISIO SARDINHA GARCIA

Sob Orientação do Professor
Dr. André Luiz de Castro Leal

Dissertação de Mestrado submetida como requisito parcial para obtenção de grau de Mestre, no Curso de Pós-Graduação em Gestão e Estratégia da Universidade Federal Rural do Rio de Janeiro – UFRRJ.

Seropédica / RJ
Agosto de 2020

Universidade Federal Rural do Rio de Janeiro
Biblioteca Central / Seção de Processamento Técnico

Ficha catalográfica elaborada
Com os dados fornecidos pelo(a) autor(a)

G216p

Garcia, Aluisio Sardinha, 1976-
Proposição, aplicação e validação de um framework de avaliação de riscos, aplicado ao compartilhamento de sistemas de radiocomunicações de um órgão de segurança pública. / Aluisio Sardinha Garcia. - Rio de Janeiro, 2020.
150 f.

Orientador: André Luiz de Castro Leal.
Dissertação(Mestrado). -- Universidade Federal Rural do Rio de Janeiro, Universidade Federal Rural do Rio de Janeiro. Instituto de Ciências Humanas e Sociais. Programa de Pós-Graduação em Gestão e Estratégia., 2020.

1. Eventos de Risco. 2. Análise de Riscos. 3. Matriz de Riscos. 4. Compartilhamento de Sistemas de Radiocomunicações. I. Leal, André Luiz de Castro, 1971 , orient. II Universidade Federal Rural do Rio de Janeiro. Universidade Federal Rural do Rio de Janeiro. Instituto de Ciências Humanas e Sociais. Programa de Pós-Graduação em Gestão e Estratégia. III. Título.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
INSTITUTO DE CIÊNCIAS SOCIAIS APLICADAS – ICSA
MESTRADO PROFISSIONAL EM GESTÃO E ESTRATÉGIA – MPGE

ALUISIO SARDINHA GARCIA

Dissertação submetida como requisito parcial para obtenção do grau de **Mestre**, no Programa de Pós-Graduação em Gestão e Estratégia, da Universidade Federal Rural do Rio de Janeiro – UFRRJ.

DISSERTAÇÃO APROVADA EM: 10/08/2020

Prof. Dr. André Luiz de Castro Leal
Presidente da Banca e Orientador
Membro Interno
MPGE/UFRRJ

Prof. Dr. José Luís Braga
Membro Externo
IETEC - MG

Prof. Dr. Juliana Baptista dos Santos Franca
Membro Interno
DECOMP/ICE/UFRRJ

Prof. Dr. Maria Cristina Drumond e Castro
Membro Interno
MPGE/PPGE/UFRRJ

DEDICATÓRIA

Dedico primeiramente a Deus por não me deixar desistir dessa empreitada.

Aos professores do MPGE por estarem sempre solícitos em partilhar seus conhecimentos e se comportarem como um farol em um caminho muitas vezes desconhecidos por mim, em especial ao meu orientador, o professor Doutor André Castro pela paciência e impaciência necessárias ao andamento das orientações.

À minha carinhosa filha, Marina Tavares, à minha linda e presente esposa, Nivea Tavares, por serem meu porto seguro, sinônimos de carinho e compreensão durante a minha ausência.

Aos meus, familiares, irmãos e amigos pelo apoio, em especial aos meus pais, Manuel e Marli por sempre acreditarem e deixarem claro em minha vida a importância da educação.

Aos meus colegas de trabalho da Polícia Federal que muito enriqueceram essa pesquisa com contribuições valiosas, com uma participação maciça de 95% dos questionários respondidos em todo o Brasil, com destaque ao meu amigo Fernando Galvão pelos ensinamentos que vão além de telecomunicações, aos meus chefes diretos José Daemon e Márcio Roberto que me autorizaram e apoiaram nesse difícil caminho, e a todos, sem exceção, que insistem na labuta de telecomunicações neste valoroso órgão de segurança pública, em especial os indeléveis Agentes de Telecomunicações (ATE).

“Existem dois tipos de riscos: Aqueles que não podemos nos dar ao luxo de correr e aqueles que não podemos nos dar ao luxo de não correr.”

(Peter Drucker)

RESUMO

GARCIA, Aluisio Sardinha. **Proposição, aplicação e validação de um *framework* de avaliação de riscos, aplicado ao compartilhamento de sistemas de radiocomunicações de um órgão de segurança pública**. Seropédica:UFRRJ,2020. 150 p. Dissertação (Mestrado Profissional em gestão e Estratégia). Instituto de Ciências Sociais Aplicadas.

Essa pesquisa teve como objetivo: propor um *Framework* aplicado ao domínio do compartilhamento de sistemas de radiocomunicações, adaptado de modelos de gestão de riscos já estabelecidos, em função dos eventos de riscos levantados na pesquisa de campo, identificou-se os seus efeitos de risco, seus impactos, as probabilidades de ocorrência destes eventos de risco e seus controles; elaborar uma Matriz de Riscos, onde foi possível identificar os níveis de risco associados aos eventos de risco levantados na pesquisa; validar o *Framework* proposto de avaliação de riscos e realizar correções por meio dos dados levantados com os respondentes. Método: a presente pesquisa científica, de abordagem qualitativa e descritiva, foi realizada com os gestores de sistemas de radiocomunicações dos setores de Tecnologia da Informação (TI) da Polícia Federal. A pesquisa foi dividida em três fases: na primeira fase, realizada por meio da pesquisa bibliográfica, foram determinados os normativos usados na elaboração do *Framework*; na segunda fase, realizada por meio de um formulário *on-line* disponibilizado aos respondentes, foi possível determinar os eventos de risco, as probabilidades de ocorrência e o impacto ao ocorrer determinado evento de risco; na terceira fase, com um grupo menor de gestores da organização, procurou validar e corrigir o *Framework* proposto e os resultados dos controles obtidos. Ao final da pesquisa, após essa fase de validação, foi possível determinar a Matriz de Riscos com os fatores de avaliação dos controles com os ajustes dos especialistas participantes da validação, apresentado um *Dashboard* dos eventos de risco ao se compartilhar sistemas de radiocomunicações de forma a facilitar e direcionar a aplicação dos recursos e prioridades no tratamento dos eventos de riscos identificados.

Palavras-chave: Eventos de Risco. Análise de Riscos. Matriz de Riscos. Compartilhamento de Sistemas de Radiocomunicações.

ABSTRACT

GARCIA, Aluisio Sardinha. **Proposition, application and validation of a risk assessment framework, applied to the sharing of radiocommunication systems of a public security agency**. Seropédica: UFRRJ, 2020. 150 p. Dissertation (Professional Master in Management and Strategy). Instituto de Ciências Sociais Aplicadas.

This research had as objective: propose a Framework applied to the domain of radiocommunication systems sharing, adapted from already established risk management models, in function of the risk events raised in the field research, its risk effects were identified, their impacts, the probabilities of occurrence of these risk events and their controls; elaborate a Risk Matrix, where it was possible to identify the risk levels associated with the risk events raised in the research; validate the proposed risk assessment framework and make corrections using the data collected from the respondents. Method: this scientific research, with a qualitative and descriptive approach, was carried out with the managers of radiocommunication systems in the Information Technology (IT) sectors of the Federal Police. The research was divided into three phases: in the first phase, carried out through bibliographic research, the norms used in the elaboration of the Framework were determined; in the second phase, carried out using an online form made available to respondents, it was possible to determine the risk events, the probabilities of occurrence and the impact when a certain risk event occurs; in the third phase, with a smaller group of managers in the organization, it sought to validate and correct the proposed Framework and the results of the controls obtained. At the end of the research, after this validation phase, it was possible to determine the Risk Matrix with the evaluation factors of the controls with the adjustments of the specialists participating in the validation, presenting a Dashboard of the risk events when sharing radio systems in order to facilitate and direct the application of resources and priorities in the treatment of identified risk events.

Keywords: Risk Events; Risk Analysis. Risk Matrix. Sharing Radiocommunication Systems.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

ABNT - Associação Brasileira de Normas Técnicas

ANATEL - Agência Nacional de Telecomunicações

ANEEL - Agencia Nacional de Eletricidade

ANP - Academia Nacional de Polícia

BPMN - *Business Process Management Notation*

CEE - Comissão de Estudo Especial

CGU - Controladoria-Geral da União

COSO - *Committee of Sponsoring Organizations of the Treadway Commission*

COSO-ERM - *Enterprise Risk Management - Integrated Framework*

DITEL - Divisão de Telecomunicações

EB - Exército Brasileiro

ER - Eventos de Risco

ETSI - Instituto de Padronização de Telecomunicações Europeu

FC - Fator de Avaliação dos Controles

IN - Instrução Normativa

ISO - *International Organization for Standardization*

LGT - Lei Geral de Telecomunicações

MP - Ministério Público

NI - Nível de Impacto do Risco

NP - Nível de Probabilidade do Risco

PF - Polícia Federal

PGR - Procuradoria Geral da República

PGRI - Política de Gestão de Riscos

PMBOK - *Project Management Body of Knowledge*

PMI - *Project Management Institute*

RA - Risco Alto

RB - Risco Baixo

RE - Risco Extremo

RI - Risco Inerente

RM - Risco Médio

RR - Risco residual

SESP - Secretaria de Segurança Pública

SWOT - *Strengths, Weaknesses, Opportunities e Threats*

TCLE - Termo de Consentimento Livre e Esclarecido

TCU - Tribunal de Contas da União

TI - Tecnologia da Informação

TIA - Associação da Indústria de Telecomunicações

UFRRJ - Universidade Federal Rural do Rio de Janeiro

SUMÁRIO

1. INTRODUÇÃO

Os sistemas de radiocomunicações na área de segurança pública no país se utilizam de tecnologias que possuem protocolos próprios que não se comunicam, resultando na sobreposição de diferentes redes com coberturas similares que atendem à diferentes órgãos que atuam na defesa e na segurança pública no país.

Existe a viabilidade do uso compartilhado de redes de radiocomunicações entre os órgãos de segurança pública, tendo em vista a otimização dos recursos, a unificação da gestão e os aspectos econômicos envolvidos (FREIRE; JORGE; CANDIDO, 2019).

Para se obter as vantagens do compartilhamento de redes de radiocomunicações é preciso mitigar os riscos deste compartilhamento, dentre esses riscos, é possível citar; se a rede estará disponível para todas as agências envolvidas; é preciso estabelecer protocolos de prioridades de acesso à rede no caso de operações integradas em função do acesso de maior criticidade; garantir a disponibilidade ou a restrição do acesso às informações conforme a necessidade da informação trafegada (FREIRE; JORGE; CANDIDO, 2019).

A realização da proposta de um processo de análise de riscos contribuirá para minimizar as incertezas hoje encontradas ao se compartilhar sistemas de radiocomunicações, incertezas estas colocadas por Freire, Jorge e Candido (2019), tais como: se a rede irá suportar o novo tráfego; se o sistema compartilhado será aceito e usado pelos servidores das organizações envolvidas; se a o sistema será capaz de compartimentar as comunicações dentro das organizações envolvidas e outros.

A pesquisa científica, de abordagem qualitativa e descritiva, foi realizada com os gestores de sistemas de radiocomunicações dos setores de Tecnologia da Informação da Polícia Federal nos estados, dividida em três fases: a primeira fase, por meio da pesquisa bibliográfica, foram determinados os normativos que foram usados na elaboração do *Framework*; a segunda fase, por meio de um formulário *on-line*, se identificou os eventos de risco, as probabilidades de ocorrência e o impacto ao ocorrer evento de risco estudado; a terceira fase, com gestores especialistas da organização, validou e realizou as correções do *Framework* proposto e dos resultados dos controles obtidos.

A motivação desta pesquisa está em minimizar as consequências indesejadas do compartilhamento de sistemas de radiocomunicações por meio de uma análise de riscos, com base em critérios técnicos, apoiada em um *Framework* que leva em consideração três normativas; a ISO31000 (2018) elaborado pela *International Organization for Standardization* (ISO), o Capítulo 11 do PMBOK (*Project Management Body of Knowledge*)

(2017) e Metodologia de Gestão e Riscos da Controladoria-Geral da União CGU (2018).

O compartilhamento entre sistemas de radiocomunicações, além de trazer a melhor reutilização do recurso aplicado na fase inicial do projeto, pode representar melhores resultados no que diz respeito a eficiência de redes de organizações, quando estas operam em missões integradas.

1.1. Contextualização Organizacional: O Objeto de Pesquisa

Na busca da melhor aplicação dos recursos financeiros na entrega de redes de radiocomunicações e no aperfeiçoamento de operações integradas é possível o uso compartilhado de redes entre órgãos de segurança pública (FREIRE; JORGE; CANDIDO, 2019). Segundo Zanetti (2011), a cultura do compartilhamento diz respeito não apenas ao aparato tecnológico que possibilita essa integração, mas também as práticas pelos sujeitos sociais envolvidos no compartilhamento, e que o compartilhamento não pode ser entendido apenas como um fenômeno, mas como um modo de sociabilidade resultando da convergência de vários aspectos.

Para que ocorra o compartilhamento é necessária uma evolução dos sistemas que se deseja integrar, a evolução da tecnologia e seus reflexos para o campo da Administração, demonstram como as mudanças que ocorrem nos sistemas e na tecnologia são aparentes e transformadoras. As empresas que não aprimorarem seus sistemas e processos de trabalho estarão vulneráveis frente à outras empresas e trilhando o insucesso (K. LAUDON e J. LAUDON, 2010). É importante que a empresa pense em evolução quando o assunto é tecnologia, e desta forma conseguir se manter estável e competitiva no mercado, buscando sempre inovar, pensando estrategicamente e até mesmo ampliar as áreas de atuação (K. LAUDON e J. LAUDON, 2010).

A tecnologia vem se desenvolvendo, e na área da administração, este crescimento foi considerável, proporcionou ganho na produção e na produtividade, favorecendo a otimização dos trabalhos e gerando maior concorrência. O gestor é responsável por garantir a evolução tecnológica na organização, este deve pensar em mecanismos para gerir a organização e como as mudanças serão introduzidas na empresa (K. LAUDON e J. LAUDON, 2010).

Davis e Newstrom (2001), afirmam que a tecnologia não é contínua, mas sim provém de uma série de explosões de novos desenvolvimentos. Em contrapartida, a consequência para o progresso que ela traz é que as pessoas precisam se adaptar às mudanças.

O compartilhamento de infraestrutura pode ser entendido como a utilização por terceiros de uma infraestrutura já utilizada em determinada prestação de serviços de utilidade

pública. Sua principal finalidade é a eficiência na utilização da estrutura instalada e o aumento do número de prestadores de serviços que se utilizam desta mesma infraestrutura evitando assim a duplicação da infraestrutura (NASCIMENTO, 2013).

É possível aumentar a eficiência das comunicações entre órgãos quando organizações diferentes compartilham o uso de uma mesma rede de radiocomunicações, para Freire, Jorge e Cândido (2019), as organizações com redes de tecnologias distintas, apresentam dificuldades em integrar suas comunicações quando é necessária uma comunicação em comum entre elas.

Em diversos grandes eventos que ocorreram no Brasil, a exemplo da Copa das Confederações 2013, a Jornada Mundial da Juventude 2013 com a visita do Papa, a Copa do Mundo 2014 e as Olimpíadas Rio 2016, existiu a necessidade da integração de comunicação entre os diversos órgãos de segurança, cenários onde três ou mais organizações participavam de uma mesma missão. Pode-se citar como exemplo, a segurança de chefes de estado que tinham a segurança aproximada formada por equipes da Polícia Federal, equipes de motociclistas chamadas de batedores que podiam ser formadas pela Polícia Rodoviária Federal e/ou formada pelo Exército Brasileiro, para o caso concreto, atuavam três organizações no mesmo cenário, com a mesma missão, no entanto os agentes de cada organização não se comunicavam com agentes de organizações diferentes, por possuírem sistemas de comunicações diferentes.

Diversas tentativas de integração das então tecnologias instaladas ocorreram, no entanto nenhuma foi capaz de garantir a comunicação eficiente entre as diferentes tecnologias. Assumpção e Minghelli (2019) ressaltam em seu estudo a importância da comunicação em uma operação policial, a comunicação pode ser considerada tão importante como o armamento e as viaturas usadas pelos policiais.

Silva (2004) entende que a administração pública quando associada à aplicação de tecnologias como meios de aprimoramentos das atividades públicas, resultam em serviços com maior valor e menor custo.

O objetivo da execução de uma atividade pública é oferecer à sociedade um serviço eficiente, com resultados positivos e que tragam retorno à sociedade. No que concerne a inovação tecnológica no âmbito dos processos da Administração Pública, Silva (2004) explica que as inovações podem acontecer na gestão da administração pública em processos, sistemas e práticas dos gestores ao criarem condições para os servidores prestarem serviços à sociedade. Os impactos que as inovações tecnológicas geram à Administração Pública apresentam efeitos positivos para ambos os lados: Estado e sociedade.

O autor dessa pesquisa, como coordenador operacional de radiocomunicações da

Polícia Federal nestes grandes eventos no Rio de Janeiro, vivenciou cenários onde forças de segurança com tecnologias de comunicação diferentes necessitaram se comunicar, mas não foi possível devido a essa barreira tecnológica criada pela não integração de tecnologias.

Considerando que o campo do compartilhamento de sistemas de radiocomunicações de órgãos de segurança tem suas consequências pouco estudadas e conhecidas no país, as inovações tecnológicas favorecem e geram impactos positivos nos setores públicos e privados. No âmbito público, as mudanças viabilizam a qualidade nos serviços prestados e como consequência a percepção pelo cidadão vem crescendo constantemente e os resultados são consideravelmente crescentes, uma vez que atinge um número maior de pessoas, tendo em vista a característica da Administração Pública, bem como de suas responsabilidades (SILVA,2004).

1.2. Situação Problema

A necessidade das diferentes organizações de segurança pública se comunicarem é cada vez mais frequente. No entanto, no cenário atual, cada organização possui um sistema de radiocomunicação próprio e estes sistemas normalmente não se interconectam.

O uso da rede de radiocomunicações pode ser compartilhado entre os órgãos de segurança pública, além da racionalização de custos sugerida por Freire, Jorge e Cândido (2019) é possível aumentar a eficiência das comunicações quando existe a necessidade de organizações diferentes se comunicarem por um objetivo comum num determinado cenário operacional.

No entanto, as organizações não direcionam seus esforços em compartilhar sistemas existentes, o cenário que se assiste na atualidade, caminha na direção de cada organização instalar seu próprio sistema pelas desconfianças colocadas por Freire, Jorge e Cândido (2019) no seu estudo, o que contribui para a importância de se realizar uma análise de riscos e elaborar um *Framework* específico, com base em modelos de gestão de riscos existentes, propondo um recorte adaptado destes processos à realidade do compartilhamento de sistemas de radiocomunicações. Nesta direção, o presente estudo procura responder à seguinte pergunta de pesquisa:

Qual a arquitetura de um Framework[1] de avaliação de riscos para suportar o compartilhamento de sistemas de radiocomunicações de um órgão de segurança pública a partir de modelos de riscos já estabelecidos?

1.3. Justificativa e Relevância

Para Nascimento (2013), o campo do compartilhamento de redes se mostra cada vez mais relevante devido as diferentes organizações se comunicarem com o passar do tempo com maior frequência entre si. No entanto, segundo Freire, Jorge e Cândido (2019), para o caso de redes de radiocomunicações de segurança, cada organização possui um sistema diferente de outras organizações e estes sistemas normalmente não se comunicam.

As observações apontadas por Jorge, Freire e Cândido (2019) a respeito da operacionalização do compartilhamento entre sistemas de radiocomunicações, reforçam que o processo de avaliação de riscos pode aumentar as chances de sucesso do compartilhamento entre sistemas de forças de segurança pública. A avaliação de riscos contribui para a identificação de prováveis cenários que irão sugerir determinados tratamentos de forma antecipada aos efeitos dos riscos levantados.

Para o PMBOK (2017), após a identificação dos riscos e análises, deve-se preparar uma resposta aos riscos por meio de um planejamento ao desenvolver ações para diminuir as ameaças e aumentar as oportunidades aos objetivos pretendidos.

Para a ISO31000 (2018), a análise de riscos é um dos processos de gestão de riscos e auxilia as organizações na tomada de decisões fundamentadas e no estabelecimento de estratégias. Ao analisar esses riscos, pode-se estudar possíveis falhas ao compartilhar sistemas de radiocomunicações e corrigi-las com antecedência, o que tornará mais aceitável o compartilhamento entre sistemas de radiocomunicações de organizações de segurança pública.

A relevância da pesquisa está no estudo do risco associado ao compartilhamento de sistemas de radiocomunicações entre forças de segurança pública e justifica-se na realização da proposta de um *Framework* de avaliação de riscos deste compartilhamento.

A proposição de um *Framework* de avaliação de riscos aplicado ao domínio do compartilhamento de sistemas de radiocomunicação contribuirá para a viabilidade do compartilhamento, com a criação de cenários de riscos, em função dos eventos de riscos

[1] Alvim(2010,p12) afirma que o *Framework* é um conjunto de classes que colaboram entre si proporcionando melhores práticas de desenvolvimento e diminuição à repetição de tarefas. Além disso, evita variações de "soluções diferentes para um mesmo tipo de problema".

levantados na pesquisa de campo, seus efeitos de risco, os impactos e as probabilidades de ocorrência destes eventos de risco.

Um dos prováveis caminhos a ser tomado, é o compartilhamento de estruturas de redes ao invés de cada órgão criar sua própria rede, a racionalização dos recursos financeiros e a busca de uma comunicação mais eficiente entre diferentes órgãos de segurança pública e defesa deve caminhar no mesmo sentido das diretrizes de uma governança pública mais eficiente.

Ao investir em inovação e nas tecnologias de informação, de forma planejada, Silva (2004), afirma que, investe-se também na qualidade do serviço prestado e na qualidade do atendimento prestado ao cidadão. A qualidade pode ser alcançada pelo uso adequado dos recursos tecnológicos.

1.4. Proposta de Solução

Para a solução do problema de pesquisa, foi proposto um *Framework* de Análise de Riscos construído a partir de três normativas: A Metodologia de Gestão de Riscos da CGU (2018); o capítulo 11 do PMBOK (2017) de gerenciamento de riscos do projeto e a ISO31000 (2018).

A realização da proposta de um processo de análise de riscos contribuirá para minimizar as incertezas encontradas quando se avalia as possibilidades e consequências do compartilhamento entre sistemas de radiocomunicações entre as organizações de segurança pública.

Ao se realizar esta análise de riscos do compartilhamento de redes de radiocomunicações, buscou identificar os riscos, analisar os riscos e avaliar os riscos diante de suas probabilidades e seus impactos ao compartilhar redes de radiocomunicações, este estudo será uma importante ferramenta na tomada de decisões dos gestores quando se deverá considerar as possibilidades do compartilhamento de redes de radiocomunicações entre organizações de segurança pública.

1.5. Objetivo Geral

Propor, aplicar e validar um *Framework* de avaliação de riscos aplicado ao compartilhamento de sistemas de radiocomunicações de um órgão de segurança pública, a partir de modelos de avaliação de riscos já estabelecidos.

1.6. Objetivos Específicos

Procurando detalhar os processos necessários para atingir o objetivo geral, serão definidos os objetivos específicos de forma a direcionar e delimitar metas a serem atingidas durante a pesquisa, neste viés pode-se definir os objetivos específicos como atividades de menor grandeza que pretendem dar suporte para se alcançar o objetivo geral.

São considerados objetivos específicos desta pesquisa:

i) Propor um *Framework* de avaliação de riscos do compartilhamento de sistemas de radiocomunicações adaptado de modelos de gestão de riscos já estabelecidos, porém aderente às necessidades do seu domínio de aplicação;

ii) Elencar, a partir da pesquisa de campo, os eventos de risco, a probabilidade e o impacto na ocorrência de determinado fator de risco e a partir da expertise do autor desta pesquisa os fatores e efeitos de risco e seus controles ao compartilhar sistemas de radiocomunicações entre órgãos de segurança pública;

iii) Realizar um estudo de interação entre os riscos identificados com seus impactos e as probabilidades de ocorrência destes riscos através da matriz de riscos classificando os eventos de risco;

iv) Validar o processo de avaliação de riscos proposto e realizar correções por meio dos dados levantados com os respondentes.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. Conceito de Compartilhamento de Infraestrutura

O compartilhamento refere-se ao aproveitamento da utilidade de uma determinada estrutura pois envolve além da atividade principal, outras atividades com utilidade pública. Neste contexto, inclui a obrigação do proprietário de redes de interconexão entre quem fornece e quem consome, dando acesso a outros prestadores que irão competir com ele (BARCELLOS, 2006).

Para Barcellos (2006), a obrigação de compartilhamento ocorre por dois motivos, a inviabilidade econômica na prestação do serviço quando da construção de infraestrutura própria ou a inexistência de meios físicos para a instalação de uma nova facilidade de modo suficiente.

O compartilhamento envolve a utilização das estruturas físicas de uma prestadora de serviços públicos por outra, tendo o objetivo de melhorar as exigências da qualidade dos serviços prestados, diante do pagamento de preços menores (KOZIKOSKI 2004).

Refere-se ao mecanismo por meio do qual se fortalece a utilidade de uma determinada estrutura, passando esta a atender outras atividades de utilidade pública além da atividade para a qual foi determinada (SUNDFELD, 2006).

Consiste na utilização da infraestrutura construída para um determinado serviço público com suporte um do outro, tendo como objetivo diminuir os custos e os valores cobrados dos usuários, deste modo contribuindo para os aspectos módicos tarifários (LAENDER, 2002; ESCOBAR, 2005). Coelho (2006) reforça ainda que no compartilhamento a rede passa a ser utilizada secundariamente em outro serviço, contribuindo então para a redução tarifária aos clientes.

2.2. O Compartilhamento de Infraestrutura na Lei Geral de Telecomunicações

A Lei Geral de Telecomunicações (LGT) desde 1997 estabeleceu que o compartilhamento de infraestrutura é obrigação e direito dos prestadores de serviços de telecomunicações de interesse coletivo. O artigo 73 da LGT preconizou que terão direito à utilização de postes, dutos, condutos e servidões controlados por prestadora de serviços de telecomunicações entre outros serviços de interesse público, de forma não discriminatória e a preços justos e razoáveis assim como as condições (BRASIL,1997).

Vale ressaltar como exemplo de aplicação do dispositivo o conteúdo da Resolução Conjunta Agência Nacional de Eletricidade (Aneel)/ Agência Nacional de Telecomunicações

(Anatel)/Agência Nacional do Petróleo nº 001, de 24 de novembro de 1999 (BRASIL,1999), a qual aprovou o Regulamento Conjunto para Compartilhamento de Infraestrutura entre agentes dos setores de energia elétrica, telecomunicações e petróleo. Sendo assim, se uma prestadora de serviços de telecomunicações requer a utilização de serviços de uma concessionária de energia elétrica para o apoio à prestação de seu serviço não pode a detentora da infraestrutura recusar o acesso pretendido a não ser que tenha uma justificativa plausível.

Cabe ressaltar também o artigo 155 da LGT, segundo o qual, "para desenvolver a competição, as empresas prestadoras de serviços de telecomunicações de interesse coletivo deverão, nos casos e condições fixados pela Agência, disponibilizar suas redes a outras prestadoras de serviços de telecomunicações de interesse coletivo" (BRASIL,1997).

Barcellos (2006, p. 3) afirma que "o compartilhamento de infraestrutura é um dos grandes desafios do Estado como ente regulador, uma vez que, em muitos casos, a infraestrutura não pode ser reproduzida por inviabilidade técnica, econômica, ambiental ou física, mesmo que tais instalações sejam essenciais para a entrada de novas prestadoras no mercado".

A LGT, por meio do artigo 155, determinou mais uma vez a todos os prestadores de serviço de telecomunicações a obrigação de compartilhar suas redes com outras prestadoras.

Sendo assim pode-se destacar a importância do poder estatal como ente regulador do setor de telecomunicações, tendo este o dever de garantir o compartilhamento de infraestrutura, viabilizando desta forma o acesso de novas operadoras no setor.

2.3. Sistemas de Radiocomunicações

A telecomunicação é uma técnica que consiste na transmissão de uma mensagem de um ponto para outro, de forma bidirecional, preservando o máximo de suas características originais. É imensurável sua abrangência e importância nos sistemas de comunicação para a economia e ciência (FOX, 2017).

A telecomunicação está presente na telefonia, internet, e-mail, satélites, óptica, redes de computadores, transmissão e processamento de imagens, cabeamentos aéreos e subterrâneos, rádio e televisão.

Para Tanenbaum (2003), protocolos de comunicação surgiram com a necessidade de interligar equipamentos empregados junto aos sistemas de automação. Para tal utilização em redes industriais é requerido modularidade, confiabilidade, interoperabilidade que é a capacidade dos sistemas abertos trocarem informações entre eles, interconectividade que é a maneira como os computadores de fabricantes diferentes podem se conectar e grande

desempenho da rede industrial.

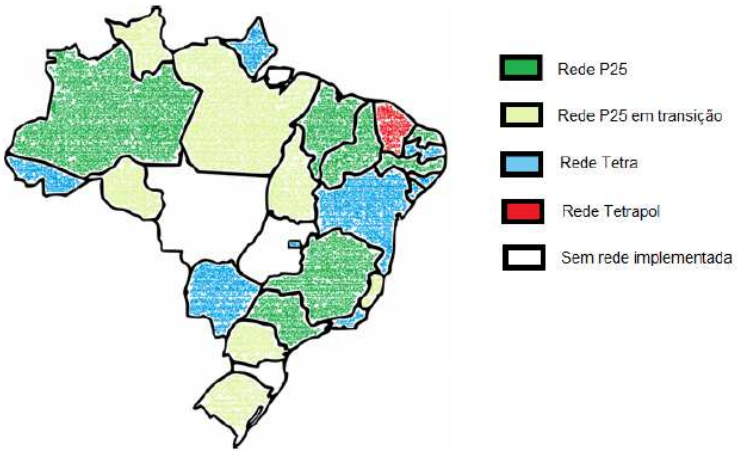
Conforme Tanenbaum (2003), os sistemas de comunicação utilizam sinais elétricos para a transmissão de informação, e são divididos em dois grandes grupos: sistema via cabo e sistema sem fio, neste último está incluído a transmissão de rádio, as radiocomunicações. Um sistema via rádio utiliza ondas eletromagnéticas como elemento de ligação entre emissor e receptor, dispensando assim meio físico.

Existem diversos critérios que influenciam na adoção dos padrões digitais, dentre eles, a qualidade técnica na transmissão e recepção dos sinais, níveis de interferência, condições de propagação, a utilização do espectro e até a compatibilidade da interoperabilidade de sinais de sistemas digitais.

Os três principais padrões de sistemas de radiocomunicação digitais usados na área de segurança no mundo são o APCO-25, o TETRA e o TETRAPOL, os quais estão sendo desenvolvidos para atender a demanda de comunicação digital na área de segurança, com as suas vantagens e desvantagens em função de suas particularidades com algo em comum: as tecnologias não se conectam (AMARAL, 2010).

A Figura 1 demostra a distribuição das redes de radiocomunicações nos estados, nas secretarias estaduais de segurança pública, qual tecnologia foi adotada por estado até o ano de 2019.

Figura 1 - Situação das redes nas secretarias de segurança públicas estaduais.



Fonte: Extraída de Freire, Jorge e Cândido, 2019.

As três tecnologias vêm sendo desenvolvidas para disponibilizar recursos e serviços no intuito de contribuir com as atividades de segurança pública. No entanto, as empresas travam uma guerra comercial na busca da expansão de suas redes, sempre com o viés da maximização dos lucros, porém ignorando a necessidade destas redes embarcadas com

tecnologia proprietária se interconectarem com as redes de outros órgãos que possuem tecnologias instaladas nas plataformas de seus concorrentes.

2.3.1. Padrões de Radiocomunicação Digital

O padrão APCO 25, também chamado de P25, refere-se à reunião de padrões da Associação da Indústria de Telecomunicações (TIA) para radiocomunicações digitais, tem sua base nos Estados Unidos das Américas (EUA) (MOTOROLA, 2010). Tem como fornecedor a Motorola, no Brasil foi absorvido na sua maioria pelo Exército Brasileiro (EB) como mostra o Quadro 1 e no campo civil pela Secretaria de Segurança Pública (SESP) do Estado de São Paulo como ilustrado na Figura 1.

O padrão TETRAPOL tem sua origem na França, tem suas especificações segundo as normas do Instituto de Padronização de Telecomunicações Europeu (ETSI) (TETRAPOL, 2011). Tem como fornecedor o grupo Airbus, no Brasil tem a sua maior rede instalada na Polícia Federal como mostra o Quadro 1, por meio de uma rede nacional que possui cobertura em todos os estados e também uma rede instalada na SESP do Ceará como ilustrado na Figura 1.

O padrão TETRA, tem a sua base na padronização do ETSI, onde inúmeras empresas fabricam e comercializam o padrão. Seu protocolo foi pensado para uso governamentais em Segurança Pública, diferentemente dos padrões anteriores, APCO 25 e TETRAPOL, não possuem desenvolvedor proprietário. Com isso recebe diversas contribuições de desenvolvimentos das mais diversas empresas ao redor do mundo por ter sido disponibilizado para domínio público pela ETSI (ETSI, 2005). No Brasil existe uma grande rede adquirida no ano de 2018 pela Polícia Rodoviária Federal de âmbito Nacional como mostra o Quadro 1, diversas secretarias de segurança do Brasil como a do Estado do Rio de Janeiro, da Bahia, do Distrito Federal e outras que utilizam o padrão TETRA ilustrados na Figura 1.

Quadro 1 - Redes nacionais x padrões instalados/instalando.

Redes Nacionais	**Padrões Instalados/Instalando**
Polícia Federal	**Tetrapol**
Exército Brasileiro	**APCO-25**
Polícia Rodoviária Federal	**Tetra**

Fonte: Elaborado pelo autor, 2019.

2.4. Modelos de Gestão de Riscos

No estudo será realizado um recorte dentro destes modelos de Gestão de Riscos no enfoque da pesquisa que é a Avaliação de Riscos.

Antes da escolha dos normativos utilizados na pesquisa, foram estudados normativos que tratavam a análise e riscos específicos da área de TI como a ISO27005 (2011), o Manual de Gestão de Riscos do Tribunal de Contas da União (TCU) (BRASIL,2018), além dos usados, a ISO31000 (2018), a Metodologia de Gestão de Riscos da CGU (2018) e o PMBOK (2017).

Suas escolhas se deram, pois, a ISO31000 (2018) é uma norma genérica aplicada à gestão de riscos, a Metodologia de Gestão de Riscos da CGU (2018) por se tratar de um normativo sistematizado e organizado usado em um órgão federal e o PMBOK por ser um guia reconhecido mundialmente em gerenciamento de projetos.

A implementação de um processo de Análise de Riscos baseado nos três normativos citados, foi baseado na busca das boas práticas de cada normativo considerando a realidade do compartilhamento de sistemas de radiocomunicações de um órgão de segurança pública.

Por ser aplicado em um domínio muito técnico e dinâmico, ainda que enxuto, quando comparado ao normativo da CGU (2018), este *Framework* demandou respostas muito céleres em função de ser aplicado em uma área da organização onde as demandas surgem a todo momento. Deste *Framework* foram exigidas respostas muito ágeis, mas que atendessem os anseios de segurança e de garantia de integridade de operação do sistema de comunicações da Polícia Federal ao se compartilhar sistemas de radiocomunicações.

Este *Framework* desenvolvido possuiu grande aderência ao normativo da CGU, até porque este é o normativo usado em gestão de riscos no qual os órgãos da esfera federal se apoiam para criarem seus próprios normativos, no entanto, o *Framework* proposto, possui fortes influências do PMBOK quando faz uso da expertise dos gestores da área de radiocomunicações da Polícia Federal como é preconizado no manual do *Project Management Institute* (PMI).

2.4.1 Riscos

Riscos são acontecimentos ou condições futuras que podem provocar impacto em um projeto ou organização tendo como consequência prejuízo ou danos. O risco é um evento ou condição incerta. Se ocorrer, terá um efeito positivo ou negativo sobre um ou mais objetivos do projeto. Vale considerar tanto a probabilidade e a frequência com a qual o risco poderá ocorrer, bem como a gravidade de suas consequências.

Caso se concretizem, poderão influenciar negativamente ou positivamente o alcance dos objetivos do projeto. Assim, cabe ao gerente do projeto identificar e monitorar, de forma contínua, as ameaças e as oportunidades que podem impactar o projeto a fim de criar estratégias que garantam a eficiência no alcance dos objetivos do projeto.

Segundo Aguiar (2011), a verificação do risco é considerada uma das tarefas de gerenciamento de projetos mais importantes, pois trata de questões para antecipação e minimização de eventos que possam impactar negativamente nos objetivos de um projeto, principalmente no que diz respeito a entidades da área governamental, onde alguns aspectos comuns nesse setor geralmente proporcionam o insucesso no gerenciamento de um projeto. Os riscos podem estar presentes em uma organização nos seguintes níveis: organização; departamento; projetos; atividades ou em situações específicas.

Um risco pode ter uma ou várias causas com impactos diversos. Se qualquer um desses riscos ocorrerem, poderá haver um impacto no custo, cronograma ou desempenho do projeto. Os aspectos relacionados ao ambiente da organização com práticas de gerenciamento de projetos contendo falhas, falta gerenciamento integrados, projetos simultâneos ou descontrole de participantes externos que fogem do controle do gerenciamento, podem contribuir para as condições de risco (AGUIAR, 2011).

2.4.2. Gerenciamento e Gestão de Riscos

O gerenciamento de riscos envolve identificar, analisar, tratar e monitorar os riscos existentes em uma organização, departamento, operação ou atividade específica. O objetivo do gerenciamento é minimizar ou até mesmo excluir a possibilidade de impactos negativos sobre os resultados esperados. Visa minimizar possíveis impactos dos riscos na organização minimizando os efeitos negativos direcionando o tratamento dos riscos que possam acontecer. Segundo o PMBOK (2017), o gerenciamento de Riscos de um projeto envolve os processos de planejamento, identificação, análise, planejamento de respostas, monitoramento e controle de riscos. Seu objetivo é maximizar os eventos positivos a fim de minimizar os efeitos negativos.

O gerenciamento de riscos é uma medida estratégica que todas as organizações deveriam utilizar. Existem várias metodologias para o gerenciamento de riscos. Dentre elas podemos destacar as diretrizes estabelecidas pela ISO31000 cujo objetivo é estabelecer princípios e orientações sobre a gestão de riscos que viabilizem o gerenciamento de vários riscos de qualquer organização.

2.4.3. ABNT NBR ISO31000

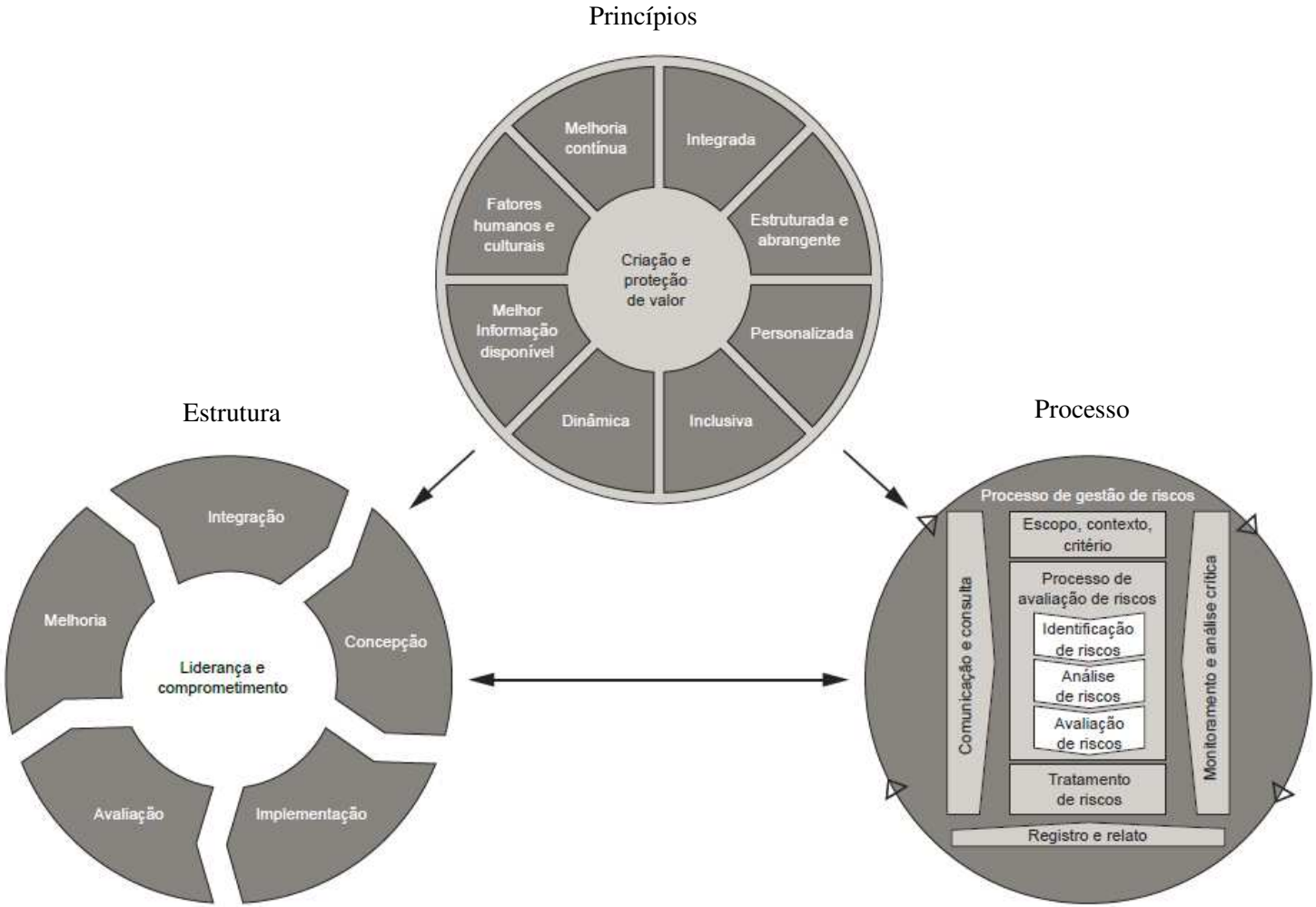
A Associação Brasileira de Normas técnicas (ABNT) ISO31000 (2018) foi elaborada pela Comissão de Estudo Especial de Gestão de Riscos (ABNT/CEE-063). É utilizada na criação e proteção das organizações, no que se refere ao gerenciamento de riscos, tomada de decisões e melhora do desempenho das organizações que a aplicam.

2.4.3.1. Contextualizando a Norma ABNT NBR ISO 31000

Segundo a ISO31000 (2018), gerenciar riscos auxilia as organizações quanto à tomada de decisões e estabelecimento de estratégias. Faz parte da governança e liderança e é importante para a forma como a organização é gerenciada em todos os sentidos e níveis, contribuindo para a melhoria dos sistemas de gestão.

Para a ISO31000 (2018), gerenciar riscos nos contextos externo e interno da organização, inclui o comportamento humano e os fatores culturais, e deste modo, baseiam-se nos princípios, estrutura e processos alinhados como demonstrado no processo macro na Figura 2.

Figura 2 - Princípios, estrutura e processo da ISO31000.



Fonte: Extraída da ISO31000, 2018.

Os princípios fornecem orientações sobre as características da gestão de riscos para que seja eficaz e eficiente, são a base para gerenciar riscos e são considerados quando se estabelecerem a estrutura e os processos de gestão de riscos da organização.

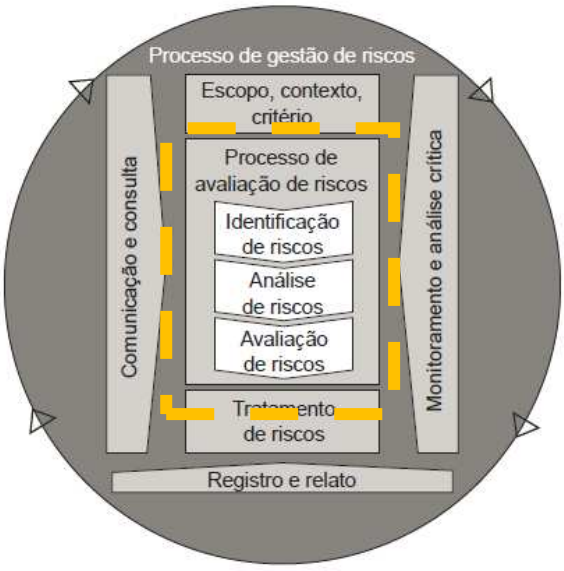
O processo de gestão de riscos envolve a aplicação de políticas e procedimentos para as atividades de comunicação e consulta, através de avaliação contínua, tratamento, monitoramento, análise crítica, registro e relato de riscos.

O recorte em estudo receberá foco dentro do Processo de Gestão de Riscos, pois nele se encontra o subprocesso de Avaliação de Riscos, objeto desta pesquisa.

2.4.3.2. Processo de Gestão de Riscos

O Processo de Gestão de Riscos, destacado na Figura 3, pode ser frequentemente apresentado como sequencial, mas na prática, para a ISO31000 (2018), não ocorre de forma sequencial. É desejável que o processo de gestão de riscos seja parte integrante da gestão da organização e da tomada de decisão, assim como esteja integrado na estrutura e nos processos da organização.

Figura 3 - Processo de gestão de riscos.



Fonte: Extraída da ISO31000, 2018.

Ainda na Figura 3 é possível identificar dentro do Processo de Gestão de Riscos os subprocessos de Comunicação e Consulta, o de Escopo, Contexto e Critério, o Processo de Avaliação de Riscos (objeto desta pesquisa), o de Tratamento de Riscos, o de Monitoramento e Análise Crítica e o de Registro e Relato.

2.4.3.3. Processo de Avaliação de Riscos

Considerando as generalidades, o processo de avaliação de riscos é o processo global de identificação de riscos, análise de riscos e avaliação de riscos. Conforme a ISO31000 (2018), é desejável que o processo de avaliação de riscos seja conduzido de forma sistemática, iterativa e colaborativa, com foco no conhecimento e nos pontos de vista das partes envolvidas e que utilize a informação disponível mais viável contendo investigação adicional.

Segundo a ISO31000 (2018), os focos da identificação de riscos são: encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus propósitos. A organização poderá usar várias formas de identificação das incertezas as quais podem afetar um ou mais objetivos. Sendo assim, segundo orientações da norma, é importante considerar: fontes tangíveis e intangíveis de risco; causas e eventos; ameaças e oportunidades; vulnerabilidades e capacidades; mudanças nos contextos externo e interno; indicadores de riscos emergentes; natureza e valor dos ativos e recursos; consequências e seus impactos nos objetivos; limitações de conhecimento e de confiabilidade da informação; fatores temporais; vieses, hipóteses e crenças dos envolvidos.

Quanto à análise de riscos, a norma ISO31000 (2018) tem por objetivo compreender a natureza e as características dos riscos. Esta análise de riscos envolve as considerações das incertezas, das fontes que contribuem com o risco, suas probabilidades, sua consequência, o cenário que está envolvido e seus controles. Neste sentido, os eventos podem ter várias causas e/ou consequências, podendo afetarem diversos múltiplos objetivos.

Sendo assim, as análises de riscos podem acontecer de diversas formas e graus de complexidade, conforme o objetivo da análise, da disponibilidade e confiabilidade da informação e do recurso disponível. Para a norma, a técnica de análise pode ser qualitativa, quantitativa ou qualitativas e quantitativas, dependendo da forma de uso.

Conforme orientações da norma, é importante que a análise de riscos considere os seguintes fatores: a probabilidade de eventos e consequências; a natureza e magnitude das consequências; complexidade e conectividade; fatores temporais e volatilidade; a eficácia dos controles existentes e a sensibilidade e níveis de confiança.

A análise de riscos pode sofrer influências das divergências de opiniões, julgamentos, à qualidade da informação utilizada, as hipóteses e as exclusões feitas, quaisquer limitações das técnicas e como elas são executadas. Segundo a norma da ISO31000 (2018), é importante que estas influências sejam consideradas, documentadas e comunicadas aos tomadores de decisão.

Quanto à avaliação de riscos, o propósito da avaliação de riscos é apoiar decisões. Envolve a comparação dos resultados da análise de riscos com os critérios de risco estabelecidos para determinar onde é importante a ação adicional. Segundo a norma, pode-se levar a uma decisão de: fazer mais nada; considerar as opções de tratamento de riscos; realizar análises adicionais para melhor compreender o risco; manter os controles existentes; e reconsiderar os objetivos. Sendo assim, é importante que o resultado da avaliação de riscos seja registrado, comunicado e assim validado nos níveis apropriados da organização.

2.4.4. Metodologia de Gestão de Riscos da CGU

No ano de 1992, a gestão de riscos em empresas tomou destaque por meio da publicação do guia *Internal Control – Integrated Framework* pelo *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), as organizações passaram a obter orientações sobre o aprimoramento de seus sistemas de controle interno. Segundo o COSO (2004), esses sistemas passaram a serem formados por componentes integrados, onde se incluiu a avaliação de riscos. Neste sentido, COSO (2004) disponibilizou o *Enterprise Risk Management - Integrated Framework - COSO-ERM*, que trazia componentes, princípios e conceitos para a gestão de riscos com enfoque no meio corporativo.

No mesmo sentido, na esfera do poder executivo federal, pode ser entendido como marco regulatório que orienta os órgãos e as entidades públicas na estruturação de mecanismos de controles internos, gestão de riscos e governança a Instrução Normativa (IN) MP/CGU nº 01, de 10 de maio de 2016 (BRASIL,2016), foram apresentados conceitos, princípios, objetivos e responsabilidades relacionados aos temas.

2.4.4.1. Contextualizando a Metodologia de Gestão de Riscos da CGU

A Metodologia de Gestão de Riscos da CGU (2018) tem o objetivo de estruturar e estabelecer as diversas etapas necessárias à operacionalização da Gestão de Riscos na CGU. Possui definido no seu art. 6º da PGR/CGU – Procuradoria Geral da República/Controladoria Geral da União, onde no mínimo, existe a necessidade das seguintes etapas que são ilustradas na Figura 4.

Possui as seguintes etapas previstas:

> I – Entendimento do Contexto: Nesta fase onde são identificados os objetivos relacionados ao processo organizacional e onde são definidos os contextos externo e interno que devem ser levados em consideração quando se pretende gerenciar riscos;
> II – Identificação de Riscos: Nesta fase são identificados possíveis riscos para objetivos associados aos processos organizacionais;

III – Análise de Riscos: são identificadas as possíveis causas e consequências do risco;

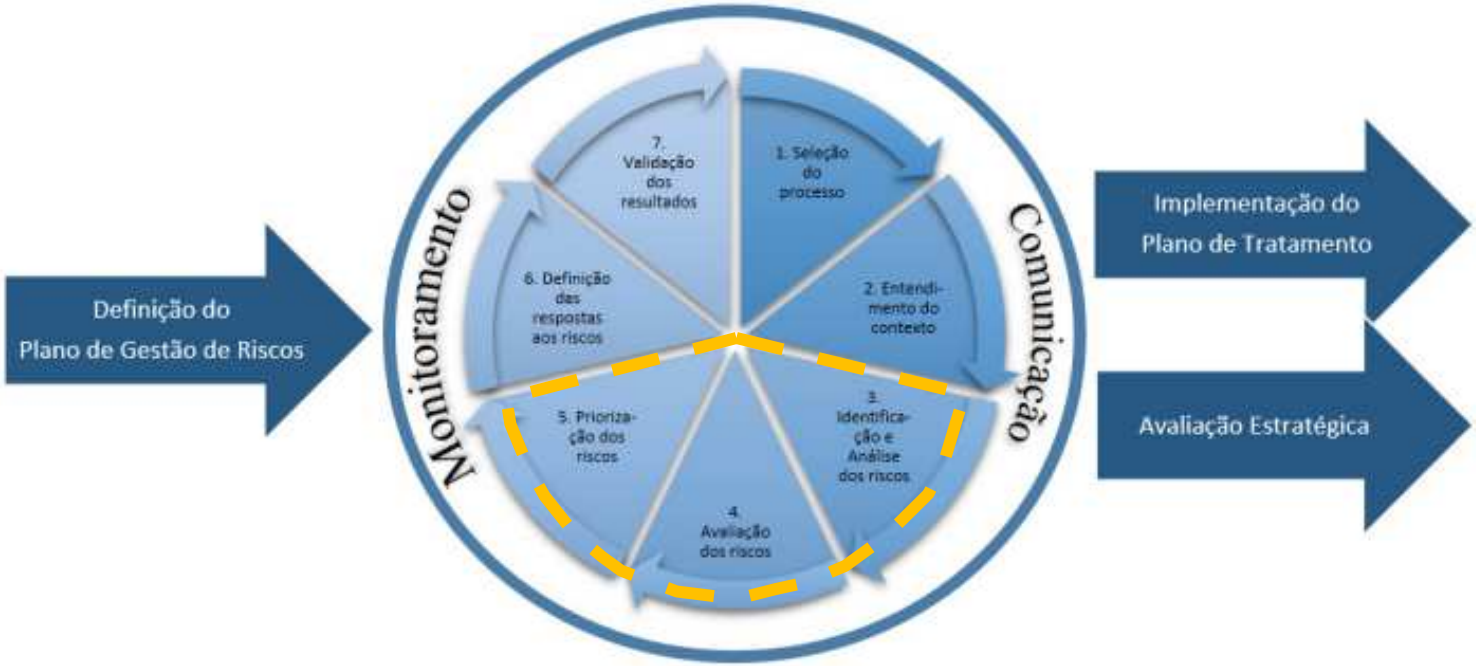
IV – Avaliação de Riscos: são estimados os níveis dos riscos identificados;

V – Priorização de Riscos: são definidos quais riscos terão suas respostas priorizadas, considerando os níveis mensurados na fase anterior;

VI – Definição de Respostas aos Riscos: são definidas as respostas aos riscos, sendo adequadas em seus níveis conforme determinado nos processos organizacionais. É importante considerar também a escolha das medidas de controle relacionando a essas respostas; e

VII – Comunicação e Monitoramento: fase que acontece durante todo o processo de gerenciamento de riscos, sendo esta responsável pela integração de todas as instâncias envolvidas, inclusive o monitoramento contínuo da Gestão de Riscos, com o objetivo de alcançar melhorias.

Figura 4 - Processo de gestão de riscos segundo a CGU.



Fonte: Extraída da Metodologia de Gestão de Riscos da CGU, 2018.

É foco desta pesquisa os seguintes tópicos; identificação de riscos; análise de riscos; avaliação de riscos e a priorização de riscos.

2.4.4.2. Identificação e Análise dos Riscos

Para a Metodologia de Gestão de Riscos da CGU (2018), no processo de Identificação e Análise dos Riscos elabora-se uma lista completa referente aos possíveis eventos que podem atrasar, prejudicar ou impedir que os objetivos do processo organizacional sejam alcançados.

Segundo a Metodologia de Gestão de Riscos da CGU (2018), para se identificar os riscos, podem ser realizadas as seguintes perguntas: Quais eventos podem EVITAR o atingimento de um ou mais objetivos do processo organizacional? Quais eventos podem ATRASAR o atingimento de um ou mais objetivos do processo organizacional? Quais eventos podem PREJUDICAR o atingimento de um ou mais objetivos do processo organizacional? Quais eventos podem IMPEDIR o atingimento de um ou mais objetivos do processo organizacional?

Conforme menciona a Metodologia de Gestão de Riscos da CGU (2018), após identificados e analisados os eventos de risco ao processo, deve se levantar as seguintes informações: qual objetivo do processo organizacional impactado pelo risco e qual a Categoria do risco?

Na Metodologia de Gestão de Riscos da CGU (2018) se identifica os tipos de risco, que são apresentados no Quadro 2.

Quadro 2 - Tipos de riscos.

Risco Operacional	Eventos que podem comprometer as atividades gerais da organização, riscos associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas.
Risco legal	Eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da organização.
Risco Financeiro/orçamentário	Eventos que podem comprometer a capacidade da organização de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações.

Risco de Integridade	Eventos relacionados a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer os valores e padrões preconizados pela Organização e a realização de seus objetivos.

Fonte: Elaborado pelo autor, 2020.

Na etapa seguinte são identificados os seguintes elementos ligados a Análise de Riscos:

Causas: motivos que podem promover a ocorrência do risco;

Consequências: resultados do risco que afetam os objetivos;

Controles preventivos: controles existentes e que atuam sobre as possíveis causas do risco, com o objetivo de prevenir a sua ocorrência.

Controles de atenuação e recuperação (reativos): controles existentes executados após a ocorrência do risco com o intuito de diminuir o impacto de suas consequências.

2.4.4.3. Avaliação dos Riscos

Para esta fase são mensurados os níveis dos riscos identificados pela equipe de avaliação de riscos, a partir de critérios de probabilidade e impacto.

Para a avaliação de riscos, a Metodologia de Gerenciamento de Riscos da CGU (2018) toma como base a Tabela 1 onde mensura a probabilidade desde muito baixo até muito alta com seus pesos de 1 a 10 respectivamente.

Tabela 1 - Escala de probabilidade.

Probabilidade	Descrição da Probabilidade, desconsiderando os controles	Peso
Muito baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	5
Alta	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	8
Muito alta	Praticamente certa.	10

Fonte: Extraída da Metodologia de Gestão de Riscos da CGU, 2018.

Também para a avaliação de riscos, a Metodologia de Gerenciamento de Riscos da CGU (2018) toma como base a Tabela 2 onde também mensura o impacto desde muito baixo até muito alto com seus pesos de 1 a 10 respectivamente.

Tabela 2 - Escala de impacto.

Impacto	Descrição do Impacto nos objetivos, caso o evento ocorra	Peso
Muito baixo	Mínimo impacto nos objetivos (estratégicos, operacionais, de informação/comunicação/divulgação ou de conformidade).	1
Baixo	Pequeno impacto nos objetivos (idem).	2
Médio	Moderado impacto nos objetivos (idem), porém recuperável.	5
Alto	Significativo impacto nos objetivos (idem), de difícil reversão.	8
Muito alto	Catastrófico impacto nos objetivos (idem), de forma irreversível.	10

Fonte: Extraída da Metodologia de Gestão de Riscos da CGU, 2018.

O produto entre o nível de probabilidade (NP) e o nível de impacto (NI) resulta no nível do risco inerente (RI), que é o nível do risco sem considerar os controles que minimizam ou podem minimizar a probabilidade da sua ocorrência ou do seu impacto.

RI = NP x NI

Onde,

RI = nível do risco inerente

NP = nível de probabilidade do risco

NI = nível de impacto do risco

A Tabela 3 classifica o risco desde Risco Baixo (RB) até o Risco Extremo (RE) em função de sua Faixa correspondente, esta faixa é resultado expressado no Risco Inerente (RI) da expressão acima.

Tabela 3 - Classificação do risco.

Classificação	**Faixa**
Risco Baixo - RB	0 – 0,99
Risco Médio - RM	10 – 39,99
Risco Alto - RA	40 – 79,99
Risco Extremo - RE	80 - 100

Fonte: Extraída da Metodologia de Gestão de Riscos da CGU, 2018.

A Figura 5 demonstra os resultados prováveis da combinação das escalas de probabilidade e impacto.

Figura 5 - Matriz de riscos.

Fonte: Extraída da Metodologia de Gestão de Riscos da CGU, 2018.

A Metodologia de Gestão da CGU (2018) em sua etapa final de Avaliação dos Riscos realiza uma avaliação e verifica a eficácia dos controles internos existentes em relação aos objetivos do processo organizacional. Preconiza que é necessário verificar se os controles apontados durante a fase de Identificação e Análise do Risco no Controle Preventivo e Controle de Atenuação e Recuperação auxiliam no tratamento do risco apontado. A Tabela 4 traz os níveis de avaliação da eficácia dos controles existentes:

Tabela 4 - Níveis de avaliação dos controles internos existentes.

Nível	Descrição	Fator de Avaliação dos Controles
Inexistente	Controles Inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	1
Fraco	Controles tem abordagem ad hoc, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas.	0,8
Mediano	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas.	0,6
Satisfatório	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	0,4
Forte	Controles implementados podem ser considerados a “melhor prática”, mitigando todos os aspectos relevantes do risco.	0,2

Fonte: Extraída da Metodologia de Gestão de Riscos da CGU, 2018.

O produto entre o valor do Risco Inerente (RI) e o Fator de Avaliação dos Controles (FC) apontado na Tabela 4 resulta no nível de risco residual (RR).

RR = RI x FC, Onde:

RR = nível do risco residual

RI = nível do risco inerente

FC = fator de avaliação dos controles existentes

O valor de risco residual resultante pode alterar a classificação de risco e enquadrar o risco em uma faixa de classificação diferente da faixa anteriormente definida para o risco inerente.

2.4.4.4. Priorização dos Riscos

Para a etapa de Priorização dos Riscos, a Metodologia de Gestão de Riscos da CGU (2018) preconiza que devem ser considerados os valores dos níveis de Riscos Residuais (RR) calculados na Avaliação de Riscos onde serão identificados os riscos que serão priorizados para tratamento. Em função do Quadro 3, a atitude a ser tomada deve levar em consideração a faixa de classificação do risco residual em relação à priorização para o tratamento e quais ações devem ser adotadas em relação ao risco e suas exceções.

Quadro 3 - Atitude perante o risco para cada classificação.

Classificação	Ação necessária	Exceção
Risco Baixo	Nível de risco dentro do apetite a risco, mas é possível que existam oportunidades de maior retorno que podem ser exploradas assumindo-se mais riscos, avaliando a relação custo x benefício, como diminuir o nível de controles.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo
Risco Médio	Nível de risco dentro do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Alto	Nível de risco além do apetite a risco. Qualquer risco nesse nível deve ser comunicado ao dirigente máximo da unidade e ter uma ação tomada em período determinado. Postergação de medidas só com autorização do dirigente máximo da unidade.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo.
Risco Extremo	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pela unidade e aprovada pelo seu dirigente máximo e pelo Comitê de Gestão Estratégica.

Fonte: Extraída da Metodologia de Gestão de Riscos da CGU, 2018.

Segundo a Metodologia de Gestão de Riscos da CGU (2018), o apetite a risco pode ser considerado o nível de risco que a unidade está disposta a aceitar, define ainda que é importante que o apetite a risco seja definido no início do processo de gerenciamento de riscos.

2.4.5. PMBOK

O PMBOK (2017) possui grupos de processos de planejamento conforme a Figura 6, dentre eles existe o grupo de processo dedicado ao Gerenciamento de Riscos que é tratado no capitulo 11 dedicado ao Gerenciamento dos Riscos do Projeto. Segundo o PMBOK (2017), gerenciar riscos do projeto inclui processos que tratam da condução do planejamento, da identificação, da análise, do planejamento das respostas e do monitoramento dos riscos em um projeto. O PMBOK (2017) ressalta que estes processos são atualizados durante todo o projeto. Este estudo toma como base a sexta edição que foi disponibilizada no ano de 2017.

2.4.5.1. Contextualizando o PMBOK

Importante ressaltar que o PMBOK (2017) possui sua metodologia toda orientada a atender projetos e possui os seguintes processos conforme o Quadro 4 para o gerenciamento de riscos:

Quadro 4 – Processos de gerenciamento de riscos segundo PMBOK.

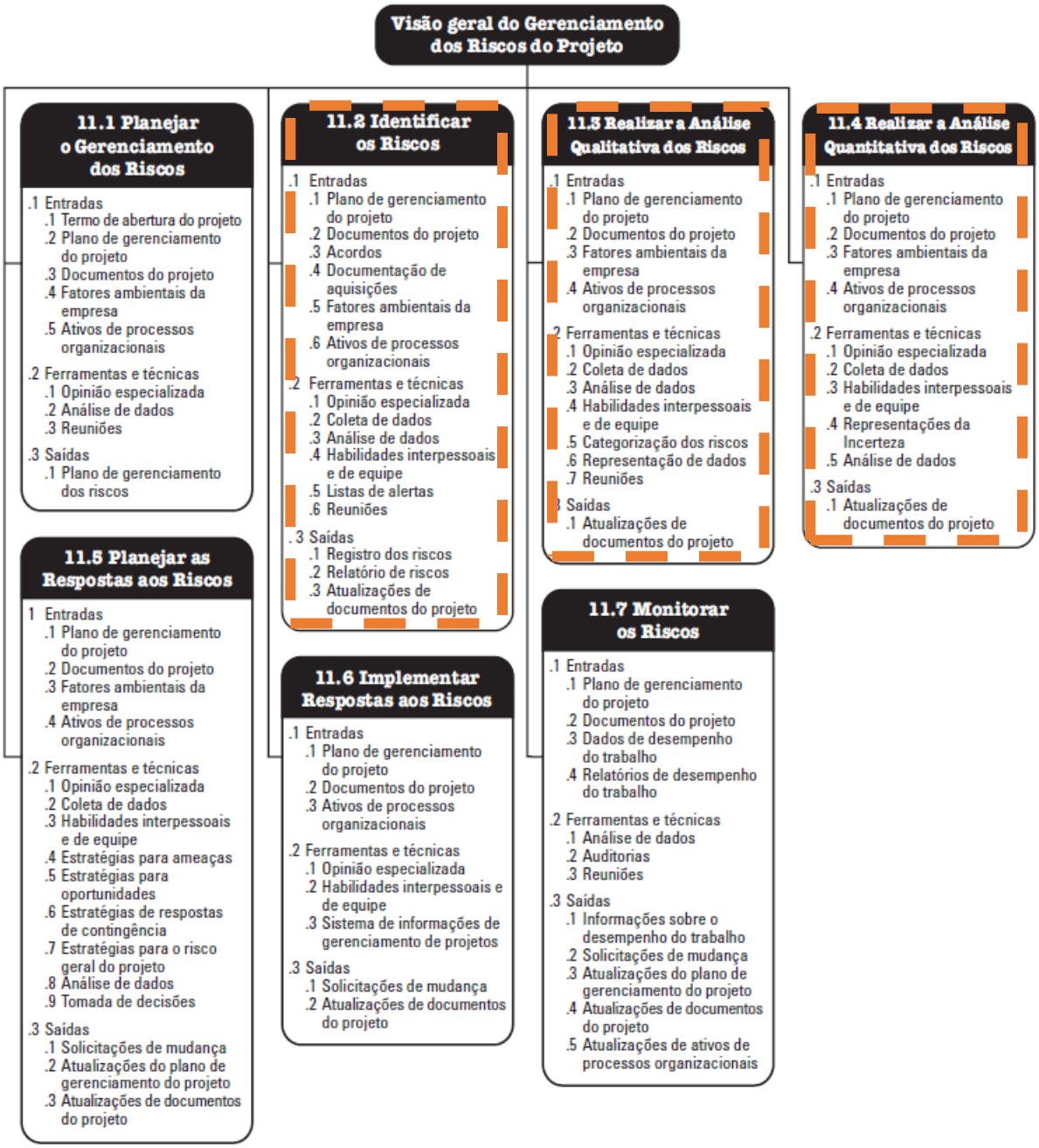
Planejamento do Gerenciamento de Riscos	Nesse processo toma-se a decisão de como abordar, planeja-se e executa-se as atividades de gerenciamento de risco como um todo para o projeto em questão.
Identificação de Riscos	Nesse processo determina-se os riscos individuais que podem afetar o projeto e documenta-se as características destes riscos.
Análise Qualitativa dos Riscos	Nesse processo, após identificado os riscos, prioriza-se os riscos para análise ou ação adicional onde se avalia e combina a probabilidade de ocorrer com o seu impacto no projeto.
Análise Quantitativa dos Riscos	Nesse processo realiza-se uma análise numérica do efeito dos riscos identificados anteriormente nos objetivos gerais do projeto.
Planejamento das Respostas dos Riscos	Nesse processo, procura-se desenvolver meios, definir estratégias e ações para lidar com a vulnerabilidade geral dos riscos e tratar os riscos individuais do projeto.

Implementar Respostas a Riscos	É o processo que procura implementar as respostas aos riscos definidas no processo anterior.
Monitoramento e Controle dos Riscos	Nesse processo é realizado o acompanhamento dos riscos identificados anteriormente, ocorre o monitoramento dos riscos residuais pós tratamento, identificação de novos riscos, nesta etapa também é executado o plano de respostas de riscos e avaliado a eficácia desse plano durante todo o ciclo de vida do projeto.

Fonte: Extraído do PMBOK, 2017.

Este estudo possui seu foco na análise de riscos. Serão utilizados os seguintes processos: Identificação dos Riscos, Realização da Análise Qualitativa dos Riscos e Análise Quantitativa dos Riscos conforme destacado na Figura 6.

Figura 6 - Visão geral do gerenciamento dos riscos do projeto.



Fonte: Extraída do PMBOK, 2017.

2.4.5.2. Identificação dos Riscos

Para o PMBOK (2017), nesta etapa procura-se identificar os riscos individuais do projeto, bem como as fontes de riscos gerais do projeto e documenta-se suas características. É um processo que é realizado ao longo do projeto por se tratar de um processo interativo pois os riscos novos surgem no decorrer do projeto.

As entradas são compostas pelo plano de gerenciamento do projeto, pelos documentos do projeto, pelos acordos, documentação de aquisições, fatores ambientais da

empresa e ativos de processos organizacionais, o PMBOK(2017) considera ainda que deve-se considerar a expertise de indivíduos ou grupos com conhecimento especializado que irão contribuir com a coleta de dados e para isso podem ser usadas técnicas como *Brainstorming*, listas de verificação, entrevistas e outros.

O PMBOK (2017) prevê como saída a conclusão do processo de identificação dos riscos. Nelas temos o conteúdo do registro dos riscos que pode incluir a lista dos riscos identificados, os possíveis responsáveis pelos riscos e a lista de possíveis respostas ao risco.

Por fim o no seu relatório final de riscos, o PMBOK (2017) sugere a apresentação das informações sobre fontes de riscos geral do projeto juntamente com informações sobre os riscos individuais identificados, além das atualizações de documentos de projeto onde retornam os registros de premissas, registros das questões, registros das lições apreendidas e outros.

2.4.5.3. Análise Qualitativa dos Riscos

O processo de análise qualitativa dos riscos, segundo o PMBOK (2017) é um processo que procura realizar a priorização dos riscos individuais do projeto, por meio de sua probabilidade e impacto de ocorrência. É um processo que também é realizado ao longo do projeto que concentra esforços em riscos de alta prioridade.

O PMBOK (2017) prevê ainda que nas entradas do processo estão os componentes do plano de gerenciamento de projetos que inclui o plano de gerenciamento dos riscos, neste processo há interesse específico nos papéis e responsabilidades no gerenciamento das atividades do cronograma, definições de probabilidade e impacto, na matriz de probabilidade e impacto e nos limites dos riscos das partes interessadas.

Fazem parte da entrada as atualizações de documentos do projeto, que segundo o PMBOK (2017) incluem o registro de premissas, o registro dos riscos, registro das partes interessadas e outros. O PMBOK (2017) lista ainda como entrada, os fatores ambientais da empresa que são os estudos setoriais de projetos e material publicado, ativos de processos organizacionais. Nas ferramentas e técnicas devem ser consideradas a opinião especializada com uso da expertise considerando projetos semelhantes anteriores e análise qualitativa dos riscos.

Na coleta de dados são utilizadas técnicas com entrevistas estruturadas ou semiestruturadas. Para o PMBOK (2017), na análise dos dados podem ser utilizadas técnicas como a avaliação de qualidade dos dados sobre os riscos, a avaliação de probabilidade dos riscos, a avaliação de outros parâmetros de riscos e outros.

Por fim, segundo o PMBOK (2017), nas saídas são realizadas atualizações de documentos do projeto, dentre eles o registro de premissas, o registro das questões, o registro dos riscos, o relatório de riscos e outros.

2.4.5.4. Análise Quantitativa dos Riscos

A análise quantitativa dos riscos, segundo o PMBOK (2017), é o processo de analisar o efeito combinado dos riscos individuais e outras fontes de incerteza, traz como principal benefício a quantificação da exposição ao risco geral do projeto.

Para o PMBOK (2017), são consideradas entradas para realizar a análise quantitativa dos riscos: o plano de gerenciamento do projeto que é composto pelo plano de gerenciamento dos riscos; linha de base do escopo; linha de base do cronograma; linha de base dos custos e outros. Ainda segundo o PMBOK (2017), também são considerados como entrada: documentos do projeto, que são compostos pelo registro de premissas; base das estimativas, estimativas de custo; previsões de custos; estimativa de duração; lista de marcos e outros.

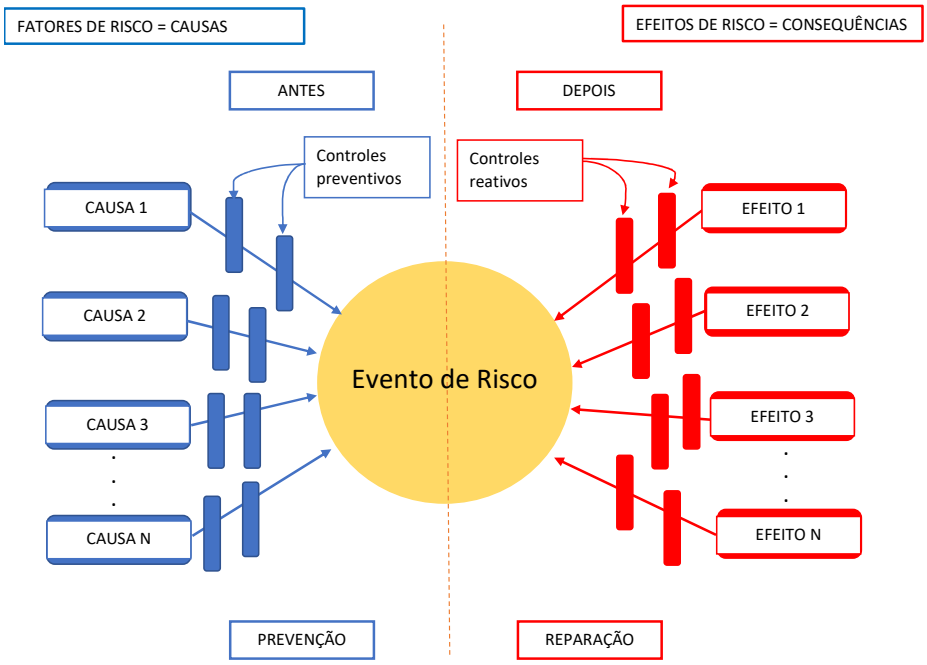
No processo de coleta de dados, o PMBOK (2017) prevê que podem ser usadas entrevistas para gerar dados para análise quantitativa dos riscos realizada com informações de especialistas. Ainda segundo PMBOK (2017), na análise dos dados, podem ser utilizadas técnicas como: a simulação; análise de sensibilidade; análise de árvore de decisão; diagrama de influência e outros.

Por fim, segundo o PMBOK (2017), são consideradas saídas para realizar a análise quantitativa dos riscos: as atualizações de documentos do projeto; dentre eles a avaliação da exposição geral ao risco do projeto; análise probabilística detalhada do projeto; a lista priorizada dos riscos individuais do projeto; as tendências nos resultados da análise quantitativa dos riscos; as respostas recomendadas aos riscos e outros.

2.5. Diagrama de *BowTie*

Para Marken (2014), a representação do diagrama *BowTie* fornece uma visão geral de forma clara dos cenários de riscos assim como a identificação de causas e efeitos destes riscos, tendo como ponto central o acontecimento crítico, que é o evento de risco. Este diagrama serve de base para uma avaliação do risco representado. A Figura 7 é apresentada para entendimento do conceito do diagrama de *BowTie*.

Figura 7 - Diagrama *BowTie*.



Fonte: Elaborada pelo autor, 2020.

O seu nome provém da semelhança do diagrama com um laço "borboleta", adquirindo a designação de diagrama *BowTie*. Constituído por duas partes, este diagrama demonstra a junção de uma árvore de falhas e uma árvore de efeitos. Esta junção permite uma identificação das causas e efeitos relacionados com o risco. Este risco é representado no ponto central do diagrama (acontecimento crítico – evento de risco).

Do ponto de vista central, na construção do diagrama é possível observar do lado esquerdo os diversos acontecimentos que proporcionam o risco em si, as causas, e do lado direito, as diferentes repercussões que tais causas possam vir a ter, os efeitos do risco.

Na constituição do Diagrama *BowTie* existe ainda a representação das barreiras de segurança, o que permite identificar a sua existência e a área de atuação. Tais barreiras incluem barreiras de prevenção e de proteção. As barreiras de prevenção (controle de preventivo), encontram-se na parte esquerda, entre os perigos e o evento de risco, as barreiras de proteção (controle reativo) encontram-se na parte direita entre o evento de risco e os efeitos. Em caso de falha nas primeiras barreiras, estas conduzem ao evento de risco e as barreiras de proteção podem ter ou não um outro evento como resultado final e sua principal função é mitigar os efeitos. Neste sentido, este diagrama permite uma rápida visualização de qual barreira de segurança é acionada em cada evento de risco identificado (KUROWICKA, et al, 2008).

Em resumo, a aplicação do método de análise *BowTie* é realizada considerando os

seguintes passos:

1. O evento de risco é identificado para análise e é representado como ponto central no diagrama;
2. As causas (fatores de risco) do evento de risco são listadas, colocando-as do lado esquerdo do diagrama;
3. Traçam-se as linhas entre a causa e o evento de risco;
4. Os controles preventivos são identificados e colocados entre a causa e evento de risco, formando o lado esquerdo do diagrama *BowTie*;
5. As prováveis consequências (efeitos de risco) do evento de risco identificado são listadas, colocando-as no lado direito do diagrama;
6. Traçam-se as linhas entre as prováveis consequências do evento de risco;
7. Os controles reativos são identificados e colocados entre o evento de risco e os efeitos de risco, formando o lado direito do diagrama *BowTie*;

3. METODOLOGIA DA PESQUISA

3.1. Caracterização da Pesquisa

A presente pesquisa científica, de abordagem qualitativa e descritiva, foi realizada com os gestores de sistemas de radiocomunicações dos setores de Tecnologia da Informação (TI) da Polícia Federal nos estados e no Distrito Federal.

As pesquisas descritivas têm como objetivo principal descrever as características de uma população ou fenômeno e até mesmo estabelecer relações entre variáveis. A pesquisa qualitativa responde a questões particulares através de diversos significados, atitudes, crenças e valores, correspondendo a um espaço mais profundo das relações e dos fenômenos que não podem ser reduzidos às questões objetivas e quantificáveis (GIL, 2002; MARCONI; LAKATOS, 2006).

Segundo Gil (2002, p. 42), "as pesquisas descritivas têm como objetivo primordial a descrição das características de determinada população ou fenômeno ou, então, o estabelecimento de relações entre variáveis".

Para Marconi e Lakatos (2006, p. 271), a pesquisa qualitativa "responde a questões particulares", (…) "ela trabalha com o universo de significados, motivos, aspirações, crenças, valores, atitudes, o que corresponde a um espaço mais profundo das relações, dos processos e dos fenômenos que não podem ser reduzidos à operacionalização de variáveis. "

A pesquisa qualitativa é realizada através do universo de significados, motivos, aspirações, crenças, valores e atitudes, considerando as relações, os processos e os fenômenos (MINAYO,1994).

Minayo (1994) explica que a pesquisa qualitativa responde a questões particulares, considerando um nível de realidade que não pode ser quantificado e nessa perspectiva se depara com um universo de significados. As interrogações vão sendo discutidas durante o próprio curso da investigação. O autor formula e reformula hipóteses, buscando compreender as mediações e correlações entre os vários objetos de reflexão e análise. Minayo (1994) destaca ainda que "é comum usar o termo "pressupostos para falar de parâmetros básicos que permitem encaminhar a investigação empírica qualitativa".

A pesquisa qualitativa não trabalha apenas com comprovações estatísticas, mas justamente pela amplitude e relevância das explicações e teorias, mesmo que estas não sejam as explicações finais e não sejam abrangentes em relação aos resultados alcançados (DUARTE, 1998).

Em uma pesquisa de cunho qualitativo, a técnica de análise deve atender a

formulação do problema a ser investigado. Sendo assim deve-se tanto sugerir perguntas como indicar possibilidades de interpretação, sendo este um referencial para os resultados que serão observados (LUNA 2000).

Para Mason (1997) a pesquisa qualitativa destaca-se pelo seu poder de fornecer a interpretação dos dados, o emprego de métodos flexíveis ao contexto no que se refere ao tratamento dos fenômenos. Já Monteiro (1991) considera como aspectos importantes da pesquisa qualitativa: "a interpretação de dados predominantemente descritivos, a supremacia do processo sobre o produto e a atenção especial conferida aos significados dos processos sociais."

3.2. Fases da Pesquisa

A pesquisa possuiu três fases bem definidas, para cada fase existiram fontes diferentes de dados e diferentes formas de tratamento dos dados.

Para melhor compreensão, a pesquisa foi dividida em três fases, são elas: primeira fase da pesquisa - Modelar o Processo; segunda fase da pesquisa - Aplicar o Processo e a terceira fase da pesquisa - Validar o Processo.

3.2.1. Modelar o Processo

Esta fase da pesquisa está concentrada em modelar o processo de compartilhamento de sistemas de radiocomunicações entre forças de segurança pública, para isso, foram estudadas normativas da área de Análise de Riscos e definidas quais foram as normativas utilizados na pesquisa.

Ainda era parte de modelar o processo, definir como seriam montados os processos e desenhá-lo de forma que melhor representasse o modelo.

3.2.1.1. Universo

Normativas estabelecidas de análise de riscos.

3.2.1.2. Critérios de Inclusão

Normativas que datam do ano 2005 até o ano de 2019.

3.2.1.3. Critérios de Exclusão

Frameworks de análise de riscos específicos de outras áreas.

3.2.1.4. Coleta de Dados

Para esta etapa de coleta de dados, têm-se para este estudo a pesquisa bibliográfica. Segundo Gil (1999), estas são pesquisas desenvolvidas a partir das contribuições dos diversos autores acerca de determinado assunto, mediante a consulta a livros e artigos científicos.

Foi realizado um estudo de modelos renomados usados frequentemente na análise de riscos, foram estudas bibliografias como a ISO27005 (2011), a ISO31000 (2018), a Metodologia de Gestão de Riscos da CGU (2018), o PMBOK (2017), o Manual de Gestão de Riscos do TCU (BRASIL,2018) e outras.

3.2.1.5. Análise de Dados

Dos modelos estudados, foram elencados três modelos para serem usados como base na criação deste processo de análise de riscos ao se compartilhar sistemas de radiocomunicações, são eles, a ISO31000 (2018), a Metodologia de Gestão de Riscos da CGU (2018) e o capítulo 11 do PMBOK (2017) que trata das etapas do gerenciamento de riscos.

Após um estudo destes modelos, foi proposto um Macroprocesso de Análise de Riscos Aplicado ao Compartilhamento de Sistemas de Radiocomunicações de Órgãos de Segurança Pública, modelo este resultante de um recorte dos processos de avaliação de riscos estudados.

Para a definição do Macroprocesso, foram usadas parte de cada normativo e definido a divisão dos subprocessos que iriam compor o Macroprocesso de Compartilhamento de Sistemas de Radiocomunicações.

O processo resultante será apresentado por meio da notação *Business Process Management Notation* (BPMN).

3.2.2. Aplicar o Processo

Esta fase da pesquisa está focada em aplicar o processo, para isso serão buscados dados com os respondentes de forma que seja possível identificar os eventos de risco, a probabilidade e os efeitos de risco ao ocorrer determinados eventos de risco.

A técnica de pesquisa empregada foi a entrevista para o levantamento dos dados que serão aplicados ao macroprocesso definido anteriormente, concluindo cada etapa dos subprocessos que compõe o macroprocesso.

3.2.2.1. Universo

Os setores de TI da Polícia Federal nos estados da federação, o órgão central de

telecomunicações em Brasília da Polícia Federal e os setores que possuam atividades de telecomunicações da Polícia Federal em Brasília.

3.2.2.2. Participantes da Pesquisa

Os participantes da pesquisa serão os servidores da rede de radiocomunicações dos setores de TI dos estados, da divisão central de telecomunicações da Polícia Federal em Brasília e dos setores que possuam atividades de telecomunicações da Polícia Federal em Brasília.

Por se tratarem os respondentes de servidores da Polícia Federal, todos eram maiores de 18 anos.

3.2.2.3. Critérios de Inclusão

Gestores que atuam na gestão da área de radiocomunicações na Polícia Federal em todo o Brasil.

3.2.2.4. Critérios de Exclusão

Servidores que estão na área de radiocomunicações há menos de um ano no órgão.

3.2.2.5. Considerações Éticas

O projeto foi apresentado ao Comitê de Ética em Pesquisa da UFRRJ e todos os respondentes concordaram com o TCLE (Termo de Consentimento Livre e Esclarecido) nos moldes do sugerido pelo Comitê de Ética da UFRRJ. Os respondentes somente seguiam com a pesquisa caso concordassem com o TCLE apresentado anteriormente as perguntas do formulário. Na Figura 8 é apresentado parte do TCLE disponibilizado aos respondentes, estes ao concordarem com o TCLE da pesquisa seguiam com a pesquisa e caso não concordassem eram direcionados para uma página onde finalizava a pesquisa.

Figura 8 - Formulário de pesquisa – Termo de Consentimento Livre Esclarecido (TCLE).

Fonte: Elaborada pelo autor, 2019.

Todos os gestores que concordaram em participar da pesquisa, deram o aceite no Termo de Consentimento Livre e Esclarecido e receberam informações a respeito da pesquisa, dentre elas: de que a participação no estudo não era obrigatória; a pesquisa não oferecia riscos aos respondentes; a preservação do sigilo de tudo aquilo que for dito e do anonimato de cada um, conforme disposto na Resolução 466/2012 do Conselho Nacional de Saúde (BRASIL, 2012), que estabelece normas de pesquisa envolvendo seres humanos.

3.2.2.6. Coleta de Dados

A coleta ocorreu por meio de um formulário *on-line* disponibilizado aos servidores através de um link do *Google Forms*. Os resultados obtidos foram transcritos no MS-Excel e apresentados na forma de tabelas, quadros e figuras.

Os respondentes ao preencherem o instrumento de coleta de dados que estava relacionado ao macroprocesso de avaliação de riscos ao compartilhar um sistema de radiocomunicações, este macroprocesso, composto por três subprocessos; a identificação dos

riscos, a análise e avaliação dos riscos e a priorização dos riscos. Sendo assim, de posse destas respostas, será possível identificar os riscos apontados pelos respondentes, analisar seus impactos, suas probabilidades de ocorrer, e com isso, construir parte da avaliação de riscos.

Inicialmente foram calibrados os formulários, foram disponibilizados para apenas 5 servidores que contribuíram com a forma do formulário e levantaram novos eventos de risco que foram inseridos na lista a ser disponibilizada para os demais respondentes.

Este formulário *on-line* disponibilizado, utilizou uma escala tanto de impacto como para probabilidade para a ocorrência de determinado fator de risco ao se compartilhar redes de radiocomunicações. Essa escala tem como referência a Escala de *Likert* com cinco pontos (COSTA et al., 2018) Dentre os quatro tipos de escalas existentes; escala nominal, escala ordinal, escala intervalar e escala da razão, usaremos a escala nominal, na qual é utilizada quando o objetivo da mensuração é classificar os dados.

Na primeira pergunta foram identificados os eventos de riscos ao se compartilhar sistemas de radiocomunicações entre órgãos de segurança pública. Por meio de uma lista os respondentes marcavam pelo menos uma das repostas, indicavam ao menos um evento de risco ao se compartilhar sistemas e radiocomunicações, importante ressaltar que, os respondentes poderiam marcar mais de um evento de risco e inclusive marcar a opção “Não existem riscos ao compartilhar sistemas de radiocomunicações”.

Existia a opção de “outros”, nessa opção o respondente apresentava um fator de risco não previsto até aquele momento e o autor da pesquisa o inseria na lista para os próximos respondentes.

Na segunda pergunta os respondentes informaram a probabilidade de ocorrência de determinado fator de risco previsto em uma lista, onde não era possível prosseguir para a próxima pergunta sem atribuir uma probabilidade a todos os eventos de risco que continham a lista.

A terceira pergunta os respondentes informaram o impacto ao ocorrer determinado fator de risco previsto em uma lista, também não era possível prosseguir para a próxima pergunta sem atribuir um valor de impacto a todos os eventos de risco que continham a lista.

Por meio dos dados dos respondentes de probabilidade e impacto, seguindo os normativos previstos para o subprocesso foram nivelados os riscos em um dos seguintes níveis de risco: Risco Baixo, Risco Médio, Risco Alto ou Risco Extremo.

Foi realizado um corte, na busca de maior relevância, onde foi considerado para as etapas posteriores os eventos de riscos que tiveram mais de 5 indicações na pesquisa de campo.

Após nivelados os eventos de risco, foram lançados na Matriz de Riscos sem o efeito dos controles de risco.

A próxima etapa foi realizada por meio do diagrama de *BowTie*, onde auxiliava na identificação dos fatores de risco (causas), os efeitos de risco (consequências), e controles de preventivos e reativos dos eventos de riscos identificados. Após identificados, foram apresentados por meio de uma tabela.

Já no subprocesso de Priorização dos Riscos, foram então avaliados os controles que foram levantados anteriormente, se estes controles eram inexistentes, fracos, medianos, satisfatórios e fortes atribuídos o seu determinado fator de controle.

Passando então os eventos de risco por um novo nivelamento onde levou em consideração os níveis atribuídos aos controles identificados.

Foi então que esses novos níveis de risco atribuídos aos eventos de risco foram lançados na matriz de riscos com os controles considerados.

3.2.2.7. Análise de Dados

Para a análise dos dados, foi utilizada uma medida de tendência central, a escala utilizada foi nominal, para Mattar (2001) em escalas nominais a única possibilidade de operação é a contagem, restando então a moda como a medida de tendência central para o caso, não sendo a adequada a média para o caso pelos motivos expostos.

Para a definição das probabilidades de ocorrência dos eventos de risco e do impacto destes eventos de risco, foram utilizados a moda das respostas dos respondentes, essa moda foi aplicada nos modelos para retornar a Matriz de Risco, tanto com aplicação do controle quanto a Matriz de Risco sem a aplicação do controle.

3.2.3. Validar o Processo

Esta fase da pesquisa será para validar o Macroprocesso de Análise de Risco elaborado junto a um grupo menor, porém de servidores ligados à alta gestão da área de telecomunicações na Polícia federal.

O processo de avaliação de riscos proposto, será validado e serão realizadas correções por meio das respostas dos participantes.

3.2.3.1. Universo

Órgão central de telecomunicações em Brasília da Polícia Federal.

3.2.3.2. Participantes da Pesquisa

Os participantes da pesquisa serão os servidores da divisão central de telecomunicações da Polícia Federal em Brasília.

Por se tratarem os respondentes de servidores da Polícia Federal, todos eram maiores de 18 anos.

3.2.3.3. Critérios de Inclusão

Servidores que atuam na gestão da área de radiocomunicações na Polícia Federal e ocupam posições estratégicas na organização na área de telecomunicações.

3.2.3.4. Critérios de Exclusão

Servidores que estão na área de radiocomunicações há menos de um ano no órgão.

3.2.3.5. Considerações Éticas

Como informado anteriormente, o projeto foi apresentado ao Comitê de Ética em Pesquisa da UFRRJ e todos os participantes assinaram o TCLE nos moldes do sugerido pelo Comitê de Ética da UFRRJ.

3.2.3.6. Coleta de Dados

A coleta de dados foi realizada a distância, por meio de sistemas de vídeo chamadas.

Para esta validação, obtivemos a participação de 3 servidores da divisão central de telecomunicações em Brasília que ocupem posição estratégica na Polícia Federal.

Foi utilizado o seguinte roteiro para validação do processo:

1 - Inicialmente foi apresentada a pesquisa;

2 - Foram apresentados os resultados da pesquisa de campo;

3 - Foi apresentada a Matriz de Riscos com os níveis de risco com os controles aplicados (Figura 22);

4 - Foi apresentada o Quadro 4 aos participantes para que validem os fatores de risco, os efeitos de risco e controles preventivos e reativos, onde, por meio de uma Escala de Likert os respondentes avaliavam os efeitos e controles como:

Discordo totalmente, Discordo, Não estou decidido, Concordo e Concordo totalmente.

5 - Foi apresentado o Quadro 7 aos participantes para que validasse os níveis dos controles internos apresentados, que definiram os fatores de avaliação dos controles dos

fatores de riscos identificados, conforme a tabela 4.

6 - Ao final foi montada a nova Matriz de Riscos com os níveis identificados após a validação dos especialistas.

3.2.3.7. Análise de Dados

As respostas serão colhidas por meio de respostas de um formulário com uso da escala de *likert*, onde serão testadas a aderência aos fatores de avaliação dos controles preventivos e reativos definidos na pesquisa no qual foram usados na Matriz de Riscos.

4. *FRAMEWORK* DE ANÁLISE DE RISCOS

4.1. Proposta de Arquitetura do *Framework*

Inicialmente, para definição da literatura a ser usada no *Framework*, foram estudadas bibliografias que tratavam a Análise de Riscos, tais como a ISO27005 (2011) que trata a gestão de riscos de segurança da informação de uma organização, o Manual de Gestão de Riscos do TCU (BRASIL,2018), a ISO31000 (2018), a Metodologia de Gestão de Riscos da CGU (2018), o PMBOK (2017) entre outras que não foram consideradas na pesquisa por sua similaridade com uma das literaturas que foram consideradas.

As normativas escolhidas foram a ISO31000 (2018), a Metodologia de Gestão de Riscos da CGU (2018) e o PMBOK (2017).

Foram escolhidos pelos seguintes motivos: a ISO31000 (2018) é uma norma internacional, genérica, aplicada à gestão riscos e elaborada por uma organização respeitada, a ISO, e possui sua última atualização em 2018; a Metodologia de Gestão de Riscos da CGU (2018) é o documento que apresenta os fundamentos e a Metodologia de Gestão de Riscos do Ministério da Transparência e da CGU, possui o objetivo de orientar as unidades a implementá-la em conformidade com a sua Política de Gestão de Riscos (PGRI), sofreu sua última atualização em 2018 e se trata de um normativo usado em órgão federal; e o capítulo 11 do PMBOK dedicado à Análise de Riscos, teve sua sexta edição em 2017, por ser um guia reconhecido em gerenciamento de projetos que traz uma padronização, identifica e conceitua processos, áreas de conhecimento, ferramentas e técnicas da gestão de projetos e foi elaborado pelo PMI que é uma das instituições de maior renome internacional em gestão de projetos.

Considerando que um dos objetivos da pesquisa foi o de desenvolver um macroprocesso de Análise de Riscos a ser validado posteriormente, a base deste macroprocesso tomou como base as três normativas já identificadas, identificou-se os processos e quais subprocessos fizeram parte deste macroprocesso de Análise de Riscos, considerou-se a maior aderência levando em consideração as características da organização em estudo e a área temática no qual se desenvolveu a pesquisa, o compartilhamento de sistemas de radiocomunicações entre órgãos de segurança pública.

O *Framework* desenvolvido possuiu grande aderência ao normativo da CGU com influências do PMBOK e ISO31000 e por ser aplicado ao compartilhamento de sistemas de radiocomunicações, extremamente técnico e dinâmico, resultou em um *Framework* enxuto com aplicação célere e com respostas rápidas.

No Quadro 5 é apresentado onde foi identificado os subprocessos em cada normativo

estudado.

Quadro 5 - Identificação de cada subprocesso por normativos.

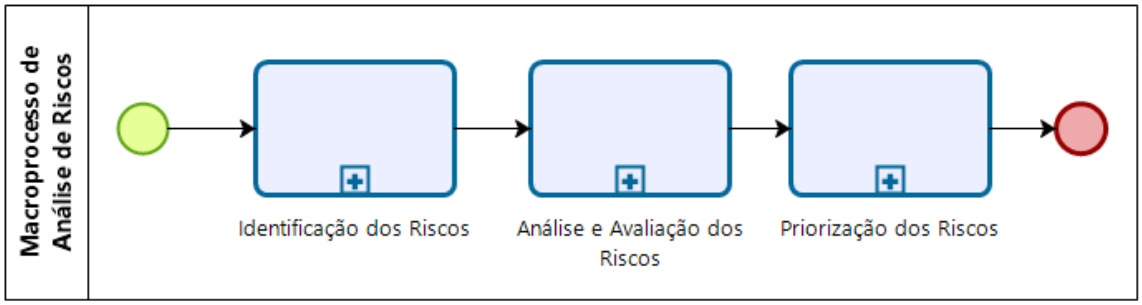
ISO 31000	CGU	PMBOCK
Identificação de Riscos	Identificação e Análise de Riscos	Identificar os Riscos
Análise de Riscos	Avaliação dos Riscos	Realizar a Análise Quantitativa dos Riscos
Avaliação dos Riscos	Priorização de Riscos	Realizar a Análise Qualitativa dos Riscos

Fonte: Elaborada pelo autor, 2019.

A aceitação da gestão por processos na cultura das empresas depende do ciclo de Gerenciamento de Processos, cuja fase inicial é a análise e modelagem de processos, a qual permite identificar, classificar e mapear os processos críticos. Neste sentido, o modelo de processo viabiliza a comunicação entre áreas de negócios e possui um mapeamento de elementos para automatizar os processos (VALLE; OLIVEIRA, 2009).

Tomando as considerações acima, foi definida a seguinte estrutura para o macroprocesso Análise de Riscos seus subprocessos como ilustrado na Figura 9.

Figura 9 - Definição do macroprocesso de Análise de Riscos e seus subprocessos.



Fonte: Elaborada pelo autor (*BPMNotation*), 2019.

Para cada um dos subprocessos criados, estes não foram necessariamente uma cópia de um subprocesso de uma das três referências escolhidas, o subprocesso resultou da mistura de dois ou de dos três subprocessos das referências adotadas para o estudo.

4.2. Proposta do Subprocesso Identificação dos Riscos

Para o PMBOK (2017) é o subprocesso que procura identificar os riscos, bem como as fontes de riscos e documentar suas características, é importante que seja realizado ao longo do projeto, pois se trata de um processo onde os riscos novos surgem no decorrer do projeto.

Para a ISO31000 (2018), este subprocesso possui o foco da identificação de riscos

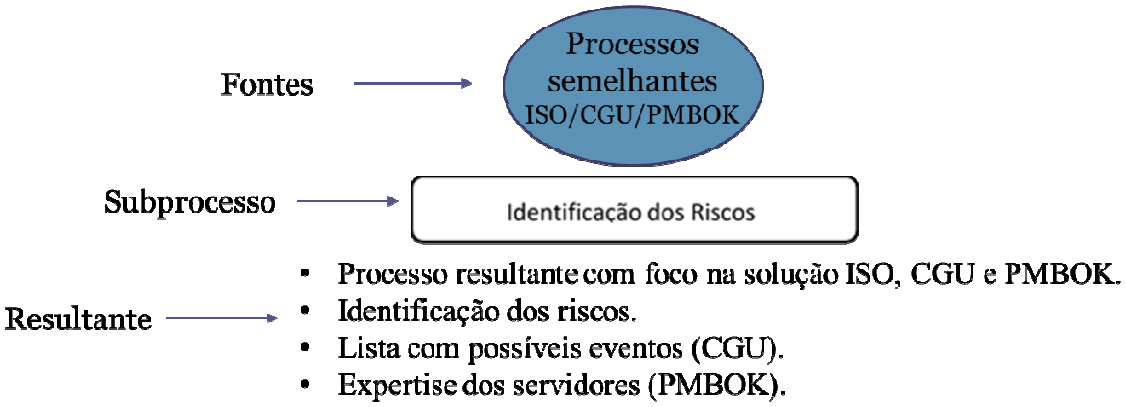
que pode ser entendida como encontrar, reconhecer e descrever riscos que ajudem ou impedem que uma organização alcance seus propósitos.

Para a Metodologia de Gestão de Riscos da CGU (2018), o subprocesso de identificação dos riscos é um subprocesso onde é elaborada uma lista que apresenta os possíveis eventos que podem atrasar, prejudicar ou impedir o que os objetivos do processo organizacional sejam alcançados ou até mesmo de suas etapas críticas, sua identificação pode ser realizada por algumas perguntas pré-definidas como apresentadas anteriormente.

O PMBOK (2017) alerta que deve ser considerado a expertise de indivíduos que irão contribuir com a coleta de dados, neste viés as entrevistas serão realizadas com os especialistas da área de radiocomunicações da Polícia Federal.

A Figura 10 apresenta as fontes do subprocesso resultante de Identificação dos Riscos, onde para esse subprocesso a identificação é tratada de forma semelhante nos três normativos. O subprocesso resultante de Identificação de Riscos fornecerá uma lista com os possíveis eventos conforme a CGU (2018) preconiza, e para essa definição dos eventos de risco são usadas a expertise dos servidores da área de gestão de radiocomunicações da Polícia Federal conforme preconiza o PMBOK (2017).

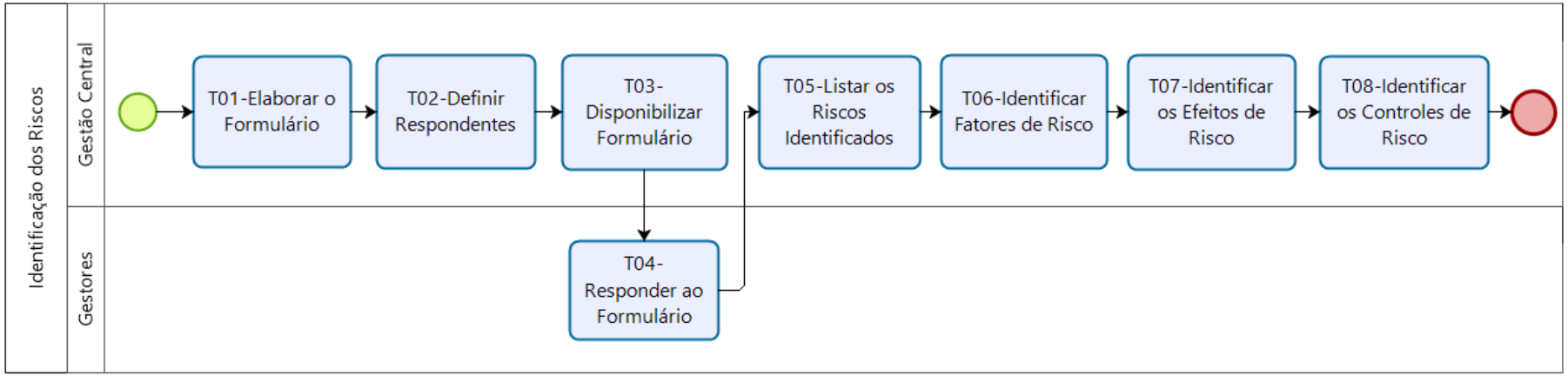
Figura 10 - Fontes x resultante do subprocesso de Identificação dos Riscos.



Fonte: Elaborada pelo autor, 2019 autor.

A Figura 11 apresenta as atividades sequenciadas que compreendem o subprocesso de Identificação dos Riscos.

Figura 11 - Definição do subprocesso de Identificação dos Riscos.



Fonte: Elaborada pelo autor (*BPMNotation*), 2020.

Onde,

T01-Elaborar Formulário: é a atividade onde é elaborado o formulário para serem passados aos gestores para a identificação dos efeitos de risco.

T02-Definir os Respondentes: é a atividade onde, com base em critérios pré-estabelecidos, se define os respondentes da pesquisa.

T03-Disponibilizar Formulário: é a atividade onde a identificação dos fatores de risco foi realizada por meio do levantamento de campo, onde um formulário *on-line* foi disponibilizado para os respondentes.

T04-Responder ao Formulário: é a atividade onde os respondentes respondem ao formulário para identificar os riscos, suas probabilidades de ocorrência e seus impactos ao ocorrerem.

T05-Listar os Riscos Identificados: é a atividade que recebe os riscos levantados pelos respondentes e cria uma lista com esses riscos.

T06-Identificar os Fatores de Risco: é a atividade onde a gestão central identifica os fatores de risco, as causas que levaram a ocorrência destes riscos, nesta pesquisa foi realizada pelo pesquisador.

T07-Identificar os Efeitos de Risco: é a atividade onde a gestão central identifica os Efeitos de Risco, as consequências da ocorrência destes riscos, nesta pesquisa foi realizada pelo pesquisador.

T08-Identificar os Controles de Risco: é a atividade onde a gestão central identifica os Controles de Risco, podendo ser controles preventivos de risco e controles reativos dos riscos, nesta pesquisa foi realizada pelo pesquisador.

Para a identificação dos fatores de riscos (causas), os efeitos de riscos (consequências) aos eventos de riscos identificados e os controles preventivos e reativos foi feito uso do diagrama *BowTie* que é uma evolução do diagrama de causa e efeito.

4.2.1. Aplicando Dados da Pesquisa ao Subprocesso de Identificação dos Riscos

4.2.1.1. Identificação dos Eventos de Risco

Após definido o Macroprocesso de Análise de Riscos e seus subprocessos, iniciou-se a etapa onde aplicamos este macroprocesso ao compartilhamento de sistemas de radiocomunicações, no caso a organização de segurança pública onde foi aplicado o processo foi a Polícia Federal.

Buscou se levantar dados como a identificação dos eventos de risco, os fatores de risco e os efeitos de risco com os gestores de radiocomunicações da Polícia Federal, para isso,

os dados de campo foram levantados buscando uma resposta ao formulário *on-line* elaborado no *Google Forms*.

Este formulário foi passado em todos os estados além do Distrito Federal, ou seja, se buscou respostas de 27 unidades, no entanto apenas em um estado não se obteve respondente. Foi disponibilizado o formulário *on-line* para 54 respondentes e se obteve 51 respostas distribuídas nos estados conforme gráfico demostrado na Figura 12.

Em Brasília conseguiu-se 8 respondentes, o Distrito Federal destoa no quantitativo dos outros estados pela sua estrutura de radiocomunicações diferenciada em relação aos estados, em Brasília a Polícia Federal possui a divisão central de telecomunicações, o setor técnico operacional voltado para o atendimento de telecomunicações em operações da PF, a ANP - Academia Nacional de Polícia com setor específico para a disciplina de comunicações, além de diretorias específicas com setores de comunicações próprios, diferente dos estados que somente possuem um núcleo de tecnologia onde se vinculam as atividades de radiocomunicações de cada estado.

Figura 12 - Respostas por estado.

Fonte: Extraída dos resultados da pesquisa de campo, 2019.

Inicialmente foram utilizados 2 dias de calibração do formulário, em dois dias de dezembro de 2019, esta calibragem foi passada para 5 servidores considerados de maior atuação da área de radiocomunicações da Polícia Federal, o chefe da Divisão de Telecomunicações (DITEL), divisão central de telecomunicações da Polícia Federal, O chefe do Setor Técnico Operacional da DITEL, um dos responsáveis da área de radiocomunicações

do estado do Rio de Janeiro, estado com a segunda maior rede de radiocomunicações do país, um representante da Bahia, estado costumeiro em apoio em operações no Brasil e um servidor responsável pela rede de radiocomunicações do Rio Grande do Sul, estado que possui uma das seis gerências da rede de radiocomunicações instaladas para controle e gerenciamento da rede nacional.

O pesquisador iniciou a calibragem com os 11 eventos de riscos identificados abaixo:

1 - A rede não suportar o tráfego de novos usuários da Polícia Federal.

2 - As informações serem perdidas.

3 - As informações perderem o sigilo.

4 - A não adaptação aos equipamentos de outra organização.

5 - Não saber manusear os equipamentos de outra organização.

6 - Os servidores se negarem a usar os equipamentos por serem equipamentos de outra organização.

7 - A Polícia Federal não adquirir os equipamentos/acessórios necessários para o uso da nova rede.

8 - A cobertura da nova rede não atender a necessidade de cobertura da Polícia Federal.

9 - A Polícia Federal não possuir prioridade da rede em situações de congestionamento.

10 - A nova rede não disponibilizar o modo tático para operações onde não haja cobertura.

11 - O Convênio de compartilhamento ser desfeito sem a devida programação.

Na etapa de calibragem além de aferidos a probabilidade de ocorrência dos riscos e o impacto dos eventos de riscos identificados pelo pesquisador listados anteriormente, foram dadas oportunidades aos respondentes para levantarem novos eventos de riscos e contribuírem com as melhorias no formulário para a busca de respostas que melhor refletissem a realidade da organização objeto da pesquisa. Pelos respondentes foram identificados e adicionados mais eventos de riscos nesta etapa de calibragem, 6 no total, e foram inseridos no formulário para serem avaliados juntos com os eventos de riscos identificados inicialmente, são eles:

12 - A gerência da rede está em outra organização.

13 - A falta de autonomia para alterar parâmetros que melhor atendem a Polícia Federal.

14 - A não possibilidade de escolha dos fornecedores. Já que os fornecedores já atendem a outra organização.

15 - A não possibilidade de fazer uso de criptografia própria.

16 - A vulnerabilidade de acesso aos centros de controle de outras organizações.

17 - Desconhecimento do pessoal que acessa os centros de controle de outras organizações.

Quanto a estrutura do formulário não se obteve observações relevantes de alteração do formulário.

O formulário em definitivo, após a calibragem, foi disponibilizado para os respondentes em dezembro de 2019, ao final de 4 dias, foram registradas 51 respostas das 54 possíveis, alcançando o índice de 94,4% de respondentes ao formulário disponibilizado.

Nesta última etapa de disponibilidade do formulário, foram identificados 4 eventos de riscos diferentes dos identificados anteriormente, chegando ao total de 21 eventos de riscos, são os 4 últimos listados abaixo:

18 - A não capacitação para a rede ser compartilhada

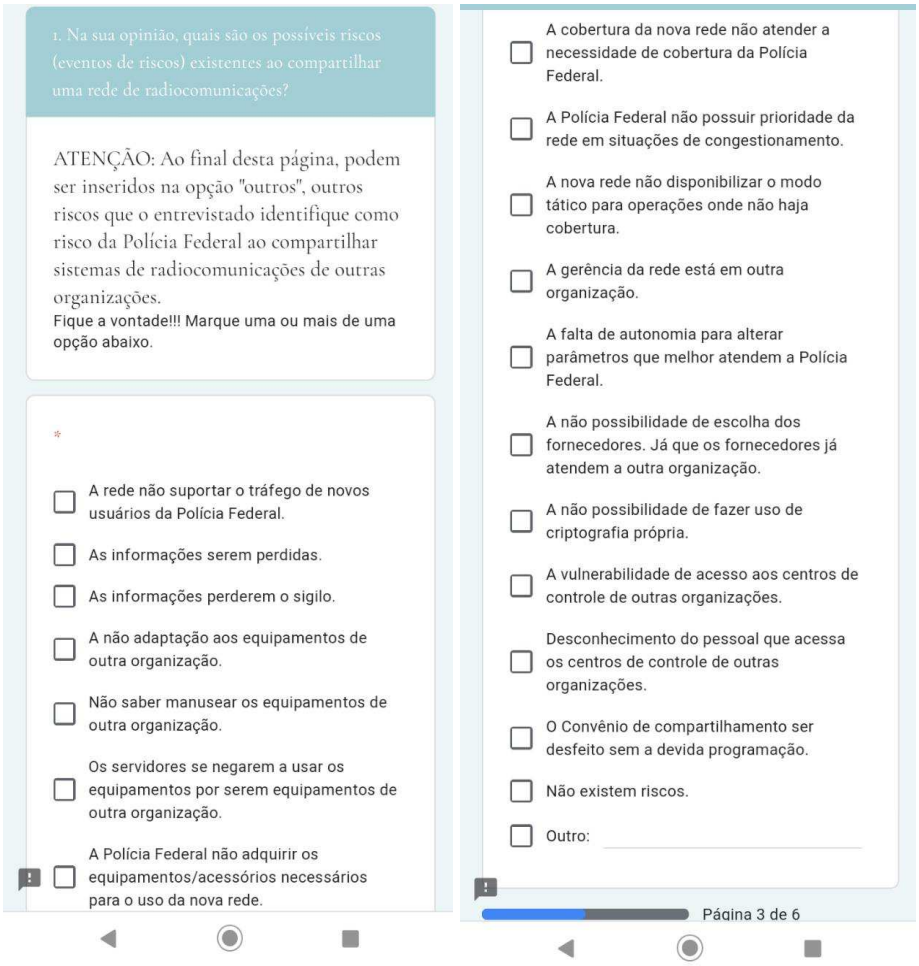
19 - A falta de manutenção da rede compartilhada

20 - Desconhecimento da tecnologia usada

21 - Desconhecimento da Segurança da Rede

No formulário *on-line* foi disponibilizado uma lista de eventos de riscos conforme Figura 13, onde nesta lista o respondente poderia selecionar mais de uma opção, indicando os eventos de risco, que no seu entendimento, existem ao compartilhar sistemas de radiocomunicações com outros órgãos de segurança.

Figura 13 - Primeira pergunta do formulário *on-line* de pesquisa.



Fonte: Elaborada pelo autor, 2019.

Ao fim da pesquisa de campo foram identificados os 21 eventos de risco listados no Quadro 6, onde foi possível identificar os eventos de risco listados em função de sua fase de identificação: identificados pelo pesquisador; identificados na etapa de calibragem ou se foram identificados durante a pesquisa.

Quadro 6 - Eventos de risco.

	Eventos de Risco
1	A rede não suportar o tráfego de novos usuários da Polícia Federal.
2	As informações serem perdidas.
3	As informações perderem o sigilo.
4	A não adaptação aos equipamentos de outra organização.
5	Não saber manusear os equipamentos de outra organização.
6	Os servidores se negarem a usar os equipamentos por serem equipamentos de outra organização.
7	A Polícia Federal não adquirir os equipamentos/acessórios necessários para o uso da nova rede.
8	A cobertura da nova rede não atender a necessidade de cobertura da Polícia Federal.
9	A Polícia Federal não possuir prioridade da rede em situações de congestionamento.
10	A nova rede não disponibilizar o modo tático para operações onde não haja cobertura.
11	O Convênio de compartilhamento ser desfeito sem a devida programação.
12	A gerência da rede está em outra organização.
13	A falta de autonomia para alterar parâmetros que melhor atendem a Polícia Federal.
14	A não possibilidade de escolha dos fornecedores. Já que os fornecedores já atendem a outra organização.
15	A não possibilidade de fazer uso de criptografia própria.
16	A vulnerabilidade de acesso aos centros de controle de outras organizações.
17	Desconhecimento do pessoal que acessa os centros de controle de outras organizações.
18	A não capacitação de servidores na rede ser compartilhada
19	A falta de manutenção da rede compartilhada
20	Desconhecimento da tecnologia usada
21	Desconhecimento da Segurança da Rede
	Não existirem riscos

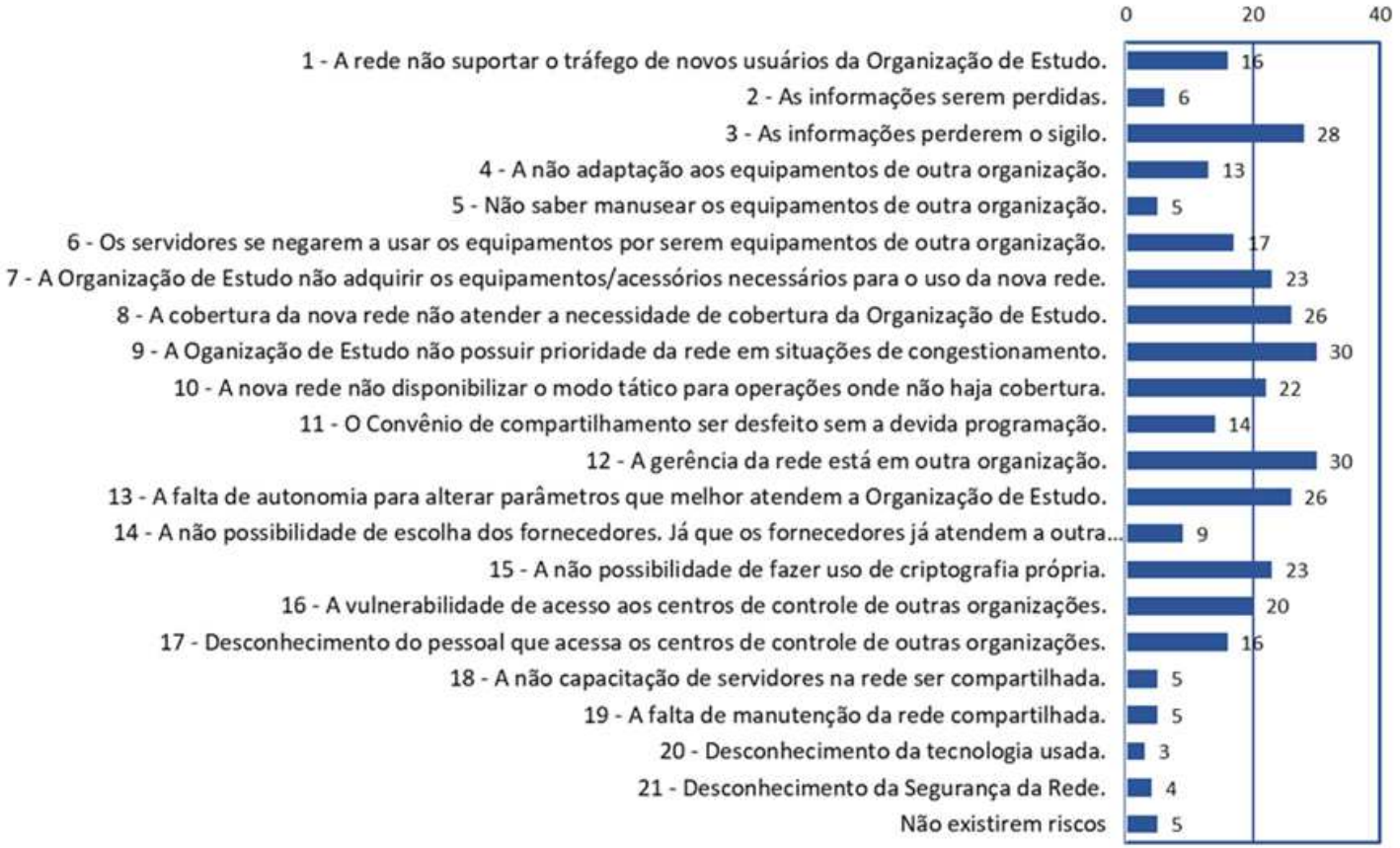
Identificados pelo pesquisador | Identificados na etapa de calibragem | Identificados durante a pesquisa

Fonte: Extraído dos resultados da pesquisa de campo, 2019.

A Figura 14 apresenta a indicação dos respondentes pelos eventos de risco disponibilizados na pesquisa, ao final foram disponibilizados vinte e um eventos de risco e os eventos de risco com maior indicação foram os eventos de risco 9 e 12 (a Polícia Federal não possuir prioridade da rede em situações de congestionamento e a Gerência da rede está em outra organização), cada um destes eventos de riscos receberam 30 indicações, ou seja, 56% dos respondentes indicaram que existem esses eventos de risco ao compartilhar redes de radiocomunicações.

Além dos eventos de riscos identificados existiram respondentes que fizeram a opção de “Não existirem riscos”, por acreditar que não existem riscos ao compartilhar redes de radiocomunicações.

Figura 14 - Indicação dos Eventos de Risco pelos respondentes na pesquisa de campo.



Fonte: Extraída dos resultados da pesquisa de campo, 2019.

4.2.1.2. Identificação dos Fatores de Risco, Efeitos de Risco e seus Controles.

É importante além de identificar os eventos de riscos, identificar as causas, chamadas de fatores de riscos, que ocasionaram determinado evento de risco (ER) e os efeitos de risco causados pelos eventos de riscos identificados.

Para a organização da identificação dos fatores de risco, seus efeitos e seus controles preventivos e reativos usamos o diagrama de *BowTie*, que como dito antes, é uma evolução do diagrama de causa e efeito, este diagrama possui o objetivo de fornecer uma visão geral, onde o ponto central é o evento de risco, e de forma direta auxiliar na identificação das causas e efeitos dos eventos de risco identificados.

Para a maior relevância de tratamento dos resultados, somente sofreram a identificação dos fatores e efeitos de risco, os eventos de riscos que receberam mais de 5 indicações conforme a Figura 14 desta dissertação.

No Quadro 7 foram listados para cada evento de risco os fatores de risco, os efeitos de risco, seus controles preventivos e seus controles reativos.

Quadro 7 - Identificação dos fatores e efeito de risco e seus controles.

Evento de Risco 1 - A rede não suportar o tráfego de novos usuários da Polícia Federal.			
Fatores	Poucos canais disponíveis. Muitos usuários usando a rede numa mesma região. A rede não foi planejada para ser compartilhada. Falta de manutenção da rede.	Preventivo	Instalar maior número de canais. Planejar a comunicação de operações integradas. Prever maior número de canais quando da entrada de novos parceiros na rede. Criar o ciclo de manutenção preventiva do sistema.
Efeito	Equipes incomunicáveis. Congestionamento da rede.	Reativo	Elaborar comunicação de contingência. Coordenar o fluxo prioritário de comunicação da rede.

Evento de Risco 2 - As informações serem perdidas.			
Fatores	Inoperância a rede. Perda de backup das informações. O não acesso ao core da rede.	Preventivo	Elaborar comunicação de contingência. Criação de rotinas de backups. Negociar o compartilhamento do core da rede.
Efeito	Falta de informações de uso da rede pelos usuários. Atraso nas respostas das demandas dos usuários.	Reativo	Busca acesso aos backups. Busca de dados em local fora de sistemas.
Evento de Risco 3 - As informações perderem o sigilo.			
Fatores	Acesso não autorizado nas bases do sistema. Uso de equipamentos de rádio não autorizado. Escuta não autorizado de informações da organização. Quebra da criptografia.	Preventivo	Identificação dos acessos e trocas de senhas periódicas. Possuir controle de uso de rádios dos usuários. Buscar protocolos de restrição de acesso aos dados da organização. Atualização das criptografias do sistema.
Efeito	Acesso não autorizado das informações da organização.	Reativo	Uso de códigos nas comunicações que dificultem o entendimento das informações trafegadas.
Evento de Risco 4 - A não adaptação aos equipamentos de outra organização.			
Fatores	Equipamentos diferentes dos usualmente usados. Falta de treinamento nos novos equipamentos. Falta de acessórios úteis a missão da organização. Equipamentos não adaptados a missão da organização.	Preventivo	Realizar treinamento nos novos equipamentos. Realizar treinamento nos novos equipamentos. Buscar os acessórios necessários ao cumprimento à missão da organização. Buscar equipamentos na nova rede que atendam as particularidades da organização.
Efeito	Os servidores não usarem os novos equipamentos. Busca de um sistema que atenda das necessidades da organização.	Reativo	Campanhas de uso e importância da comunicação numa organização de segurança. Continuar prospectando sistema de comunicação próprio.

Evento de Risco 6 - Os servidores se negarem a usar os equipamentos por serem equipamentos de outra organização.			
Fatores	Não adaptação aos equipamentos. Falta de treinamento. Rejeição ao uso de novos equipamentos.	Preventivo	Campanhas de uso e importância do da comunicação numa organização de segurança. Realizar treinamentos de uso dos equipamentos. Campanhas de uso e importância do da comunicação numa organização de segurança.
Efeito	Os servidores não usarem os novos equipamentos.	Reativo	Realizar treinamento nos novos equipamentos.
Evento de Risco 7 - A Polícia Federal não adquirir os equipamentos/acessórios necessários para o uso da nova rede.			
Fatores	Falta de recursos para compra dos equipamentos / acessórios. Não serem disponibilizados pelo fornecedor equipamentos / acessórios de acordo com a particularidade da organização.	Preventivo	Buscar orçamento justificando a necessidade do recurso para compra dos equipamentos / acessórios que atendam a necessidade da organização. Buscar com outros fornecedores equipamentos / acessórios que atendam a necessidade da organização.
Efeito	Os servidores não usarem os novos equipamentos.	Reativo	Campanhas de uso e importância do da comunicação numa organização de segurança até que se busque os equipamentos/acessórios que atendam a necessidade da organização.
Evento de Risco 8 - A cobertura da nova rede não atender a necessidade de cobertura da Polícia Federal.			
Fatores	Falhas de estações. Não previsão dos locais que interessam a organização nos projetos de instalação.	Preventivo	Buscar orçamento justificando a necessidade do recurso para compra dos equipamentos / acessórios que atendam a necessidade da organização. Buscar com outros fornecedores de equipamentos / acessórios que atendam a necessidade da organização.
Efeito	Falta de cobertura nos locais de atuação da organização. Os servidores não usarem os novos equipamentos.	Reativo	Buscar junto ao gestor da rede a instalação de novas estações de transmissão que atendam a organização. Campanhas de uso e importância da comunicação numa organização de segurança até que se obtenha coberturas que atendam a necessidade da organização.

Evento de Risco 9 - A Polícia Federal não possuir prioridade da rede em situações de congestionamento.			
Fatores	A não previsão de prioridade da rede no projeto de instalação do sistema. Falta de disponibilidade de canais de comunicação.	Preventivo	Solicitar junto ao gestor da rede a prioridade dos canais. Aumento do número de canais da rede.
Efeito	Os servidores não conseguirem usar a rede de comunicação.	Reativo	Busca de um sistema de comunicação de contingencias.
Evento de Risco 10 - A nova rede não disponibilizar o modo tático para operações onde não haja cobertura			
Fatores	O sistema não disponibilizar sistema tático. A Polícia Federal não adquirir o sistema tático.	Preventivo	Buscar um sistema de contingencias que supra o modo tático Realizar estudos para a compra do sistema tático.
Efeito	Falta de cobertura em áreas remotas.	Reativo	Busca de um sistema de contingencias para suprir o modo tático.
Evento de Risco 11 - O Convênio de compartilhamento ser desfeito sem a devida programação.			
Fatores	Falta de gerencia dos prazos do contrato. Descumprimento dos acordos do contrato. Não atendimento das necessidades de comunicação da organização.	Preventivo	Manter os cuidados com os prazos e gerencia dos prazos junto a organização parte do contrato. Manter os cuidados para o cumprimento dos acordos contratuais da organização previstos no contrato. Buscar sistemas de contingencias e prospectar sistemas próprios de comunicação.
Efeito	Os servidores não conseguirem usar a rede de comunicação.	Reativo	Busca de um sistema de comunicação de contingencias.
Evento de Risco 12 - A gerência da rede está em outra organização.			
Fatores	A organização ser a detentora da gerência da rede. O sistema não permitir espelhamento da gerencia da rede.	Preventivo	Buscar junto à organização que gerencia a rede acesso aos controles da rede. Buscar junto à organização o espelhamento da gerencia do sistema.

Efeito	Não ser possível customizar a rede como as alterações que melhor atendem a organização.	Reativo	Buscar junto à organização que possui a gerencia da rede as possibilidades de customizar a rede para que melhor possa atender a Polícia Federal.
Evento de Risco 13 - A falta de autonomia para alterar parâmetros que melhor atendem a Polícia Federal.			
Fatores	A organização ser a detentora da gerência da rede. Não ser previsto em contrato a autonomia necessária para alterações de parâmetros que melhor atendem a Polícia Federal.	Preventivo	Buscar junto à organização que gerencia a rede acesso aos controles da rede. Buscar instruir cláusulas no contrato de compartilhamento que permitam a Polícia Federal alterar parâmetros que melhor lhe atendam.
Efeito	Não ser possível customizar a rede como as alterações que melhor atendem a organização. Os servidores não conseguirem usar a rede de comunicação.	Reativo	Buscar junto à organização que possui a gerencia da rede as possibilidades de customizar a rede para que melhor possa atender a Polícia Federal. Busca de um sistema de comunicação de contingencias.
Evento de Risco 14 - A não possibilidade de escolha dos fornecedores. Já que os fornecedores já atendem a outra organização.			
Fatores	O contrato pertencer a outra organização. A Polícia Federal não possuir interesse em ter uma rede própria.	Preventivo	Busca aproximação aos fornecedores para atender as necessidades da PF. Prospectar uma rede de radiocomunicação própria.
Efeito	Fornecedores com propostas engessadas de preço e disponibilidade de material diferenciado.	Reativo	Prover gestões junto aos fornecedores materiais que atenda a organização com preços de mercado.
Evento de Risco 15 - A não possibilidade de fazer uso de criptografia própria.			
Fatores	A criptografia já vier inserida no sistema contratado. O gerador de chaves criptográficas não ficar instalado na Polícia Federal. O sistema não possibilitar instalar criptografia própria.	Preventivo	Buscar junto à organização que gerencia o sistema a possibilidade de instalar uma criptografia própria da Polícia Federal. Buscar junto à organização que gerencia o sistema instalar na Polícia Federal o gerador de chaves criptográficas. Buscar junto aos fornecedores e ao gestor do

			sistema de comunicações os meios para instalar uma criptografia própria.
Efeito	A Polícia Federal fazer uso de uma criptografia comum na organização. Os servidores não usarem os novos equipamentos.	Reativo	Fazer uso de controle controles de segurança próprios dos equipamentos que possibilitem a customização para a atividade da Polícia Federal. Buscar de novos equipamentos que atendam a organização.
Evento de Risco 16 - A vulnerabilidade de acesso aos centros de controle de outras organizações.			
Fatores	Os centros de controle estar em outra organização. Desconhecimento dos controles aplicados pela organização que gerencia o sistema.	Preventivo	Buscar informações e combinar protocolos de acesso com a outra organização. Buscar informações e participar dos controles que existem nos centros de controle.
Efeito	As informações trafegadas pela organização estarem expostas.	Reativo	Procurar fazer uso de códigos na comunicação.
Evento de Risco 17 - Desconhecimento do pessoal que acessa os centros de controle de outras organizações.			
Fatores	Não participar da seleção de pessoas que acessam o sistema. A gestão do centro de controle não estar na Polícia Federal.	Preventivo	Buscar informações das pessoas que acessam os centros de controle. Buscar informações das pessoas que acessam os centros de controle.
Efeito	As informações trafegadas pela organização estarem expostas.	Reativo	Procurar fazer uso de códigos na comunicação.

Fonte: Elaborado pelo autor, 2020.

Os controles preventivos e reativos foram resultados da expertise do autor dessa pesquisa, posteriormente esses controles serão validados por especialistas da organização em estudo.

4.3. Proposição do Subprocesso de Análise e Avaliação dos Riscos

Para a ISO 31000 (2018), o PMBOK (2017) e a CGU (2018) os subprocessos de análise e avaliação dos riscos são tratados de forma separadas, para otimizar os processos e que estes processos se caracterizem por um entrega efetiva, os dois subprocessos foram reunidos num único processo.

Outro motivo para se unirem os subprocessos de Análise e Avaliação de Riscos é melhor explicado na Figura 15, pois nesta etapa iremos elaborar a matriz de Riscos, e a matriz é trabalhada em subprocessos diferentes como é possível observar.

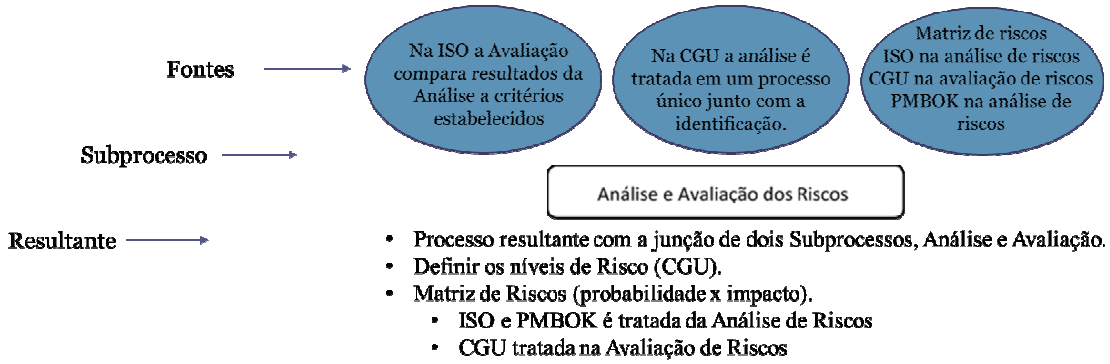
Para a ISO31000 (2018), o objetivo da análise de riscos está em compreender a natureza do risco e suas características, deve ser realizada uma análise detalhada das incertezas e fontes de risco.

Ainda segundo a ISO31000 (2018), as técnicas de análise podem ser qualitativas, quantitativas ou qualitativa e quantitativa, dependendo da forma de uso e é importante que as influências sejam consideradas, documentadas e comunicadas aos tomadores de decisão.

Já o PMBOK (2017) trata o subprocesso de análise e riscos dividido em duas análises, a análise qualitativa dos riscos e a análise quantitativa dos riscos.

Na Figura 15 são apresentadas as fontes dos subprocessos de Análise e Avaliação de Ricos, onde os níveis de risco são identificados conforme preconiza a CGU (2018), apara a Matriz de Riscos, os normativos definem o seu tratamento da mesma forma, no entanto em subprocessos diferentes nos seus normativos.

Figura 15 - Fontes x resultante do subprocesso de Análise e Avaliação dos Riscos.



Fonte: Elaborada pelo autor, 2019 autor.

No PMBOK (2017) a análise qualitativa é realizada por meio de uma priorização dos riscos onde a sua probabilidade de ocorrência e impacto é analisada na matriz de probabilidade e impacto.

Para a Metodologia de Gestão de Riscos CGU (2018), nesta fase são mensurados os

níveis dos riscos identificados na etapa anterior de avaliação de riscos, a partir de critérios de probabilidade e impacto, onde realiza um estudo de interação entre as escalas de probabilidade e impacto, resultando na Matriz de Riscos.

A Matriz de Riscos procura relacionar a probabilidade de ocorrência de determinado fator de risco com o impacto causado por este risco ao compartilhar sistemas de radiocomunicações por meio do produto impacto X probabilidade.

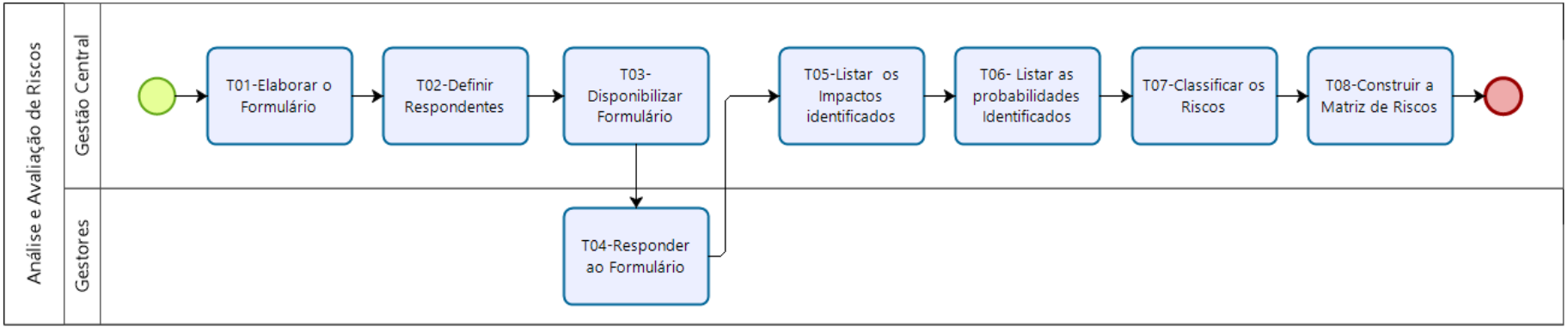
A Matriz de Riscos possibilita uma classificação dos riscos de forma rápida e direta e permite uma resposta/ação a estes visando proteger os objetivos do projeto também de forma mais rápida.

A Matriz de Riscos possui seus elementos com as quatro classificações; RE – Risco Extremo; RA – Risco Alto; RM – Risco Médio e RB - Risco Baixo conforme a Tabela 3 desta pesquisa.

Para os riscos extremos (RE), existem os riscos com alto impacto e alta probabilidade de ocorrência, nenhum projeto sobrevive com riscos em nível tão alto a longo e a médio prazo, são necessárias ações de mitigação para a "saúde" do projeto, ao passo que, para riscos baixos (RB), existem probabilidades baixas de ocorrência com baixo impacto, são riscos que são aceitáveis em seus níveis atuais, no entanto são monitorados ainda que em menor frequência. Já os riscos altos (RA), devem ser monitorados com frequência, pois se não mitigados podem resultar em efeitos tão grandes quanto os riscos extremos. Por fim os riscos médios (RM) sofrem menor monitoramento que os riscos altos e maior monitoramento que os riscos baixos, mas devem ser observados pois podem possuir impactos que prejudiquem os objetivos do projeto.

A Figura 16 apresenta o subprocesso de Análise e Avaliação dos Riscos e suas atividades sequenciadas.

Figura 16 - Definição do subprocesso de Análise e Avaliação dos Riscos.



Fonte: Elaborada pelo autor (*BPMNotation*), 2020.

Onde,

T01-Elaborar o Formulário: é a atividade onde é elaborado o formulário para serem passados aos gestores para a identificação dos efeitos de risco. Esta atividade está apenas ilustrada nesse subprocesso para sua identificação e existência, esta atividade é realizada na subprocesso de identificação de riscos.

T02-Definir os Respondentes: é a atividade onde, com base em critérios pré-estabelecidos, se define os respondentes da pesquisa. Esta atividade está apenas ilustrada nesse subprocesso para sua identificação e existência, esta atividade é realizada na subprocesso de identificação de riscos.

T03-Disponibilizar Formulário: é a atividade onde a identificação dos fatores de risco foi realizada por meio do levantamento de campo, onde um formulário *on-line* foi disponibilizado para os respondentes. Esta atividade está apenas ilustrada nesse subprocesso para sua identificação e existência, esta atividade é realizada na subprocesso de identificação de riscos.

T04-Responder ao Formulário: é a atividade onde os respondentes respondem ao formulário para identificar os riscos, suas probabilidades de ocorrência e seus impactos ao ocorrerem.

T05-Listar os Impactos Identificados: é a atividade onde se recebe os impactos aos riscos levantados pelos respondentes e identifica em uma lista os impactos para cada risco identificado.

T06-Listar as Probabilidades Identificadas: é a atividade onde se recebe as probabilidades aos riscos levantados pelos respondentes e identifica em uma lista as probabilidades para cada risco identificado.

T07-Classificar os Riscos: é a atividade onde a gestão central classifica os riscos em Risco Extremo, Risco Alto, Risco Médio e Risco Baixo em função do produto da probabilidade de ocorrência e o impacto dos riscos identificados.

T08-Construir a Matriz de Risco: é a atividade onde a gestão central constrói a Matriz de Riscos em função dos níveis riscos classificados na atividade anterior, nesta pesquisa foi realizada pelo pesquisador.

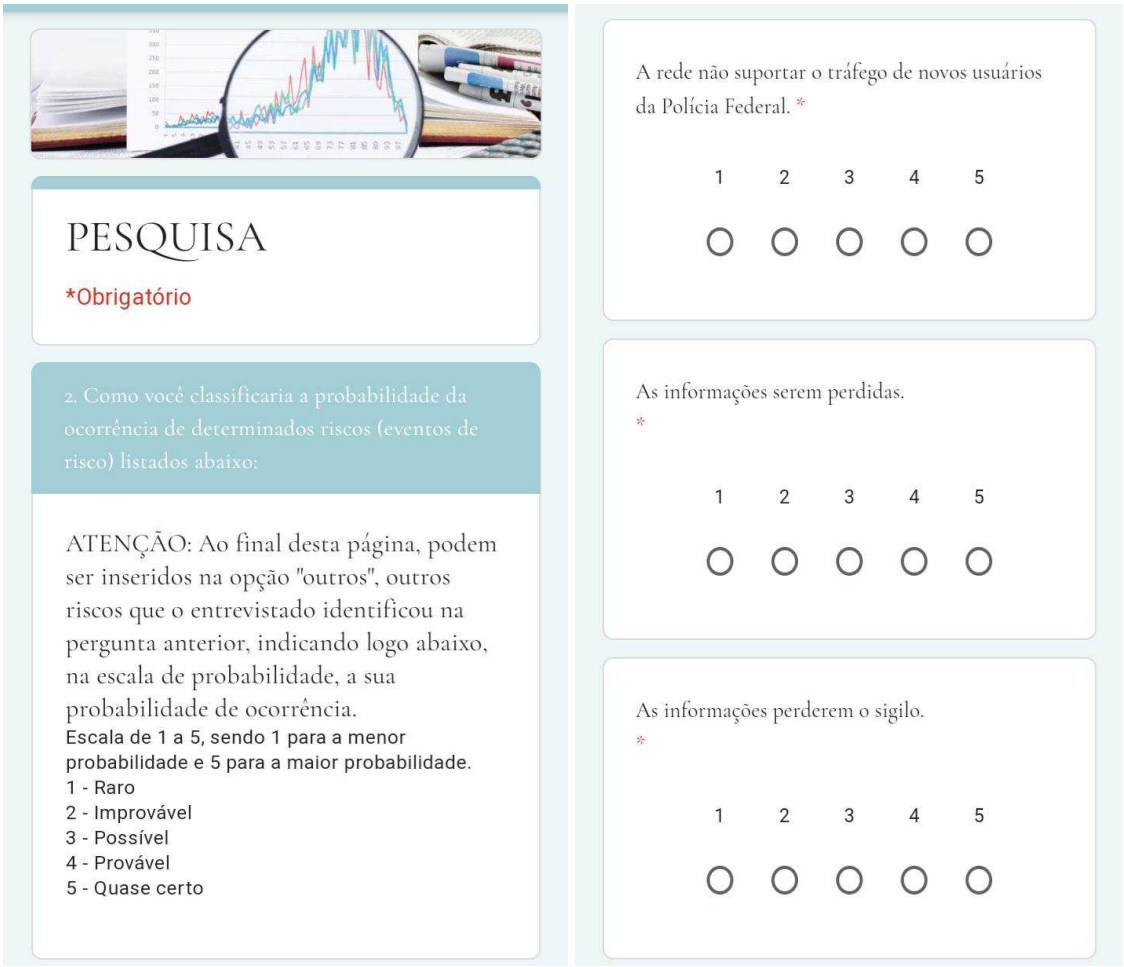
4.3.1. Aplicando Dados ao Subprocesso de Análise e Avaliação dos Riscos

4.3.1.1. Listar as Probabilidades Identificadas

A segunda pergunta respondida no formulário procurava levantar a probabilidade de ocorrência dos eventos de riscos indicados na pergunta anterior, os respondentes acessaram um formulário contendo uma lista de eventos de risco e abaixo destes eventos de risco, uma graduação para a probabilidade de ocorrência dos eventos de risco ao compartilhar sistemas de radiocomunicações a ser indicada que podia ser; 1 para raro, 2 para improvável, 3 para possível, 4 para provável e 5 para quase certo.

Na Figura 17 é apresentada a tela do formulário, como exemplo, são apresentados os três primeiros eventos de riscos da lista, e somente era possível prosseguir com o formulário se indicasse uma das probabilidades disponibilizadas para cada fator de risco.

Figura 17 - Segunda pergunta do formulário *on-line* de pesquisa.



Fonte: Elaborada pelo autor, 2019.

O Quadro 8 traz a consolidação das respostas, onde por exemplo, para o fator de

riscos 1 “ A rede não suportar o tráfego de novos usuários da Polícia Federal” foram obtidos as seguintes respostas; 9 respondentes acharam raro ocorrer o fator de risco, 10 respondentes acharam improvável o fator de risco ocorrer, 23 acharam possível o fator de risco ocorrer, 7 acharam provável o fator de risco ocorrer e 2 acharam quase certo o fator de risco ocorrer.

Na escala de *Likert* aplicada à probabilidade, são apresentados os seguintes valores; 1 para insignificante, 2 para pequeno, 3 para moderado, 4 para alto e 5 para muito alto, e quando aplicada ao impacto teremos 1 para raro, 2 para improvável, 3 para possível, 4 para provável e 5 para quase certo.

No Quadro 8 está marcada a moda em vermelho, para a probabilidade de ocorrência tomando por base a Tabela 1, chega-se ao valor a ser usado na multiplicação da probabilidade X impacto listados na coluna “Valor Matriz de Riscos” deste Quadro 8.

Quadro 8 - Seleção dos respondentes para a probabilidade de ocorrência dos eventos de risco indicados com destaque da moda.

		Pesos Tabela 1					
		1	2	5	8	10	
	Pergunta 1	Pergunta 2					Probabilidade
		Probabilidade de Ocorrência (Número de seleções)					
Eventos de Risco	Indicação do Evento de Risco	1 Raro	2 Improvável	3 Possível	4 Provável	5 Quase certo	Valor Matriz Riscos
1 - A rede não suportar o tráfego de novos usuários da Organização de Estudo.	16	9	10	23	7	2	5
2 - As informações serem perdidas.	6	9	19	17	6	0	2
3 - As informações perderem o sigilo.	28	5	8	18	13	7	5
4 - A não adaptação aos equipamentos de outra organização.	13	9	14	19	8	1	5
5 - Não saber manusear os equipamentos de outra organização.	5	11	19	11	5	5	2
6 - Os servidores se negarem a usar os equipamentos por serem equipamentos de outra organização.	17	11	9	14	7	10	5
7 - A Organização de Estudo não adquirir os equipamentos/acessórios necessários para o uso da nova rede.	23	4	9	17	11	10	5
8 - A cobertura da nova rede não atender a necessidade de cobertura da Organização de Estudo.	26	5	8	14	16	8	8
9 - A Oganização de Estudo não possuir prioridade da rede em situações de congestionamento.	30	3	8	17	16	7	5
10 - A nova rede não disponibilizar o modo tático para operações onde não haja cobertura.	22	6	7	15	19	4	8
11 - O Convênio de compartilhamento ser desfeito sem a devida programação.	14	4	11	24	7	5	5
12 - A gerência da rede está em outra organização.	30	2	4	18	13	14	5
13 - A falta de autonomia para alterar parâmetros que melhor atendem a Organização de Estudo.	26	3	9	13	19	7	8
14 - A não possibilidade de escolha dos fornecedores. Já que os fornecedores já atendem a outra organização.	9	7	9	18	8	9	5
15 - A não possibilidade de fazer uso de criptografia própria.	23	6	8	16	11	10	5
16 - A vulnerabilidade de acesso aos centros de controle de outras organizações.	20	6	6	20	14	5	5
17 - Desconhecimento do pessoal que acessa os centros de controle de outras organizações.	16	6	10	16	13	6	5
18 - A não capacitação de servidores na rede ser compartilhada.	5		1	2	2		8
19 - A falta de manutenção da rede compartilhada.	5			3	2		5
20 - Desconhecimento da tecnologia usada.	3			1	2		8
21 - Desconhecimento da Segurança da Rede.	4			2	2		8

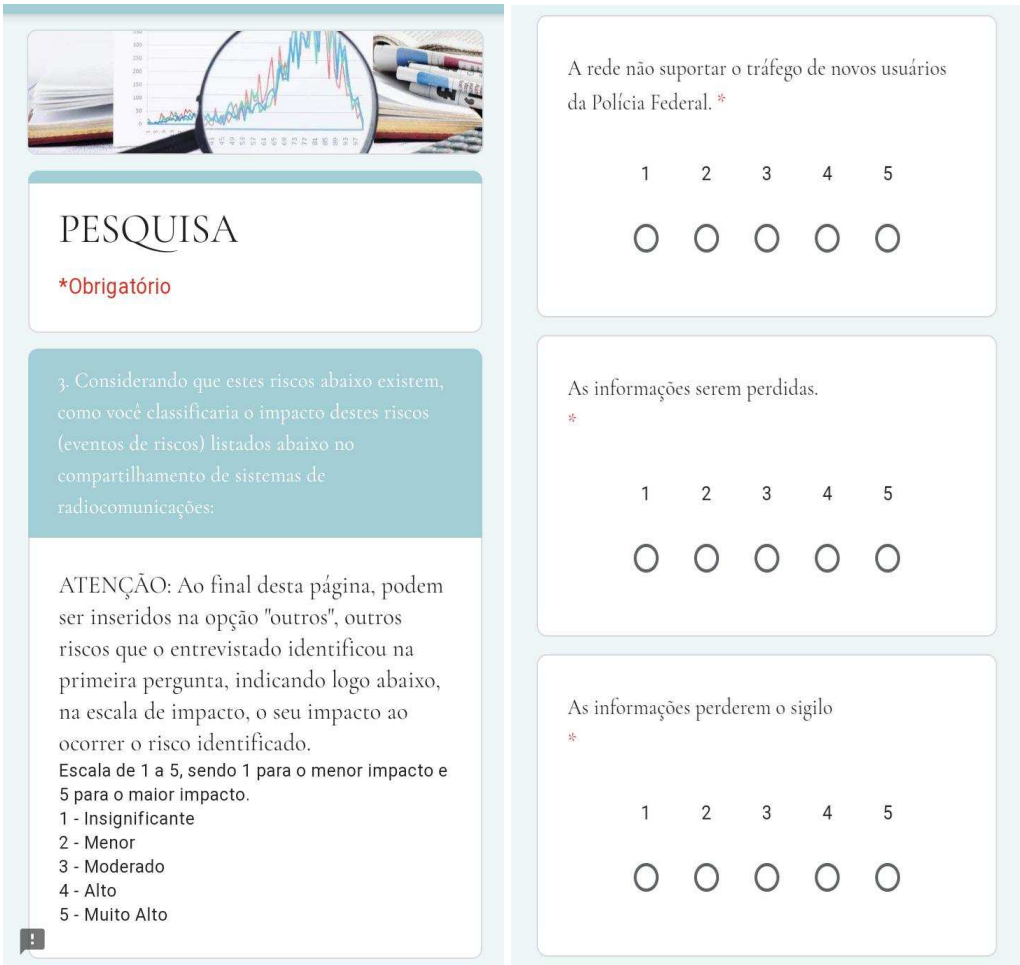
Fonte: Extraído dos resultados da pesquisa de campo, 2020.

4.3.1.2. Listar os Impactos Identificados

A terceira pergunta respondida no formulário procurava levantar o impacto para a ocorrência dos riscos indicados na primeira pergunta, para isso os respondentes possuíam no formulário uma lista de eventos de risco e abaixo destes eventos de risco uma graduação para ser indicado o impacto para ocorrência destes riscos no compartilhamento de sistemas de radiocomunicação, que podia ser; 1 para insignificante, 2 para pequeno, 3 para moderado, 4 para alto e 5 para muito alto.

A Figura 18 apresenta a tela do formulário para a terceira pergunta, como exemplo, são apresentados os três primeiros eventos de riscos da lista, onde somente era possível prosseguir com o formulário se indicasse um dos impactos disponibilizados para cada fator de risco.

Figura 18 - Terceira pergunta do formulário *on-line* de pesquisa.



Fonte: Elaborada pelo autor, 2019.

O Quadro 9 traz a consolidação das respostas, onde por exemplo para o fator de

riscos 3 “As informações perderem o sigilo” foram obtidos as seguintes respostas; 6 respondentes acharam insignificante o impacto ao ocorrer o fator de risco, 3 respondentes acharam pequeno o impacto ao ocorrer o fator de risco, 5 respondentes acharam pequeno o impacto ao ocorrer o fator de risco, 6 respondentes acharam alto o impacto ao ocorrer o fator de risco, 31 respondentes acharam muito alto o impacto ao ocorrer o fator de risco.

Ainda no Quadro 9 é apresenta a moda marcada em vermelho, para o impacto da ocorrência tomando por base a Tabela 2, chega-se ao valor a ser usado na multiplicação da probabilidade X impacto listados na coluna “Valor Matriz de riscos” deste Quadro 9.

Quadro 9 - Seleção dos respondentes para o impacto de ocorrência dos eventos de risco indicados com destaque da moda.

		Pesos Tabela 2					
		1	2	5	8	10	
	Pergunta 1	Pergunta 3					Impacto
		Impacto na ocorrencia do Risco (Número de seleções)					
Eventos de Risco	Indicação do Evento de Risco	1 Insignificante	2 Pequeno	3 Moderado	4 Alto	5 Muito Alto	Valor Matriz Riscos
1 - A rede não suportar o tráfego de novos usuários da Organização de Estudo.	16	8	2	12	18	11	8
2 - As informações serem perdidas.	6	7	7	9	14	14	10
3 - As informações perderem o sigilo.	28	6	3	5	6	31	10
4 - A não adaptação aos equipamentos de outra organização.	13	8	10	16	9	8	5
5 - Não saber manusear os equipamentos de outra organização.	5	10	16	15	6	4	2
6 - Os servidores se negarem a usar os equipamentos por serem equipamentos de outra organização.	17	4	17	11	6	13	2
7 - A Organização de Estudo não adquirir os equipamentos/acessórios necessários para o uso da nova rede.	23	5	4	13	18	11	8
8 - A cobertura da nova rede não atender a necessidade de cobertura da Organização de Estudo.	26	5	0	13	15	18	10
9 - A Oganização de Estudo não possuir prioridade da rede em situações de congestionamento.	30	5	2	10	17	17	10
10 - A nova rede não disponibilizar o modo tático para operações onde não haja cobertura.	22	5	4	4	22	16	8
11 - O Convênio de compartilhamento ser desfeito sem a devida programação.	14	4	6	12	21	8	8
12 - A gerência da rede está em outra organização.	30	10	11	17	10	3	5
13 - A falta de autonomia para alterar parâmetros que melhor atendem a Organização de Estudo.	26	3	7	7	19	15	8
14 - A não possibilidade de escolha dos fornecedores. Já que os fornecedores já atendem a outra organização.	9	4	4	15	12	16	10
15 - A não possibilidade de fazer uso de criptografia própria.	23	3	4	18	19	7	8
16 - A vulnerabilidade de acesso aos centros de controle de outras organizações.	20	7	2	13	12	16	10
17 - Desconhecimento do pessoal que acessa os centros de controle de outras organizações.	16	5	7	13	17	9	8
18 - A não capacitação de servidores na rede ser compartilhada.	5			2	3		8
19 - A falta de manutenção da rede compartilhada.	5			2	2	1	8
20 - Desconhecimento da tecnologia usada.	3		1	1	1		8
21 - Desconhecimento da Segurança da Rede.	4		1	2	1		5

Fonte: Extraído dos resultados da pesquisa de campo, 2020.

4.3.1.3. Construir a Matriz de Risco

No Quadro 10 são apresentados os valores para probabilidades e impacto retirados a partir da moda, o resultado do produto da probabilidade X impacto e a sua classificação de eventos de risco segundo a Tabela 3, onde RB – Risco Baixo, RM – Risco Médio, RA – Risco Alto e RE – Risco Extremo.

É importante ressaltar, conforme Tabela 1 e Tabela 2, os pesos que possuem cada classificação, para probabilidade 1 para raro, 2 para improvável, 5 para possível, 8 para provável e 10 para muito alto e para o impacto os pesos 1 para insignificante, 2 para pequeno, 5 para moderado, 8 para alto e 10 para muito alto.

Quadro 10 - Valores do produto da probabilidade X impacto e sua classificação.

	Probabilidade	Impacto		
Eventos de Risco	Valor Matriz Riscos	Valor Matriz Riscos	Produto Prob x Imp	Classificação
1 - A rede não suportar o tráfego de novos usuários da Organização de Estudo.	5	8	40	RA
2 - As informações serem perdidas.	2	10	20	RM
3 - As informações perderem o sigilo.	5	10	50	RA
4 - A não adaptação aos equipamentos de outra organização.	5	5	25	RM
5 - Não saber manusear os equipamentos de outra organização.	2	2	4	RB
6 - Os servidores se negarem a usar os equipamentos por serem equipamentos de outra organização.	5	2	10	RM
7 - A Organização de Estudo não adquirir os equipamentos/acessórios necessários para o uso da nova rede.	5	8	40	RA
8 - A cobertura da nova rede não atender a necessidade de cobertura da Organização de Estudo.	8	10	80	RE
9 - A Oganização de Estudo não possuir prioridade da rede em situações de congestionamento.	5	10	50	RA
10 - A nova rede não disponibilizar o modo tático para operações onde não haja cobertura.	8	8	64	RA
11 - O Convênio de compartilhamento ser desfeito sem a devida programação.	5	8	40	RA
12 - A gerência da rede está em outra organização.	5	5	25	RM
13 - A falta de autonomia para alterar parâmetros que melhor atendem a Organização de Estudo.	8	8	64	RA
14 - A não possibilidade de escolha dos fornecedores. Já que os fornecedores já atendem a outra organização.	5	10	50	RA
15 - A não possibilidade de fazer uso de criptografia própria.	5	8	40	RA
16 - A vulnerabilidade de acesso aos centros de controle de outras organizações.	5	10	50	RA
17 - Desconhecimento do pessoal que acessa os centros de controle de outras organizações.	5	8	40	RA
18 - A não capacitação de servidores na rede ser compartilhada.	8	8	64	RA
19 - A falta de manutenção da rede compartilhada.	5	8	40	RA
20 - Desconhecimento da tecnologia usada.	8	8	64	RA
21 - Desconhecimento da Segurança da Rede.	8	5	40	RA

Fonte: Extraído dos resultados da pesquisa de campo, 2020.

Na matriz de riscos é possível observar um código de cores para o resultado deste produto, verde para risco baixo, amarelo para risco médio, laranja para risco alto e vermelho para risco extremo, valores estes que tomam por base a Tabela 3.

Os eventos de risco (ER) são inseridos então com o seu código correspondente (ERn), onde n corresponde ao código dado ao evento de risco de 1 a 21, na matriz de risco possibilita uma melhor visualização dos riscos que merecem um tratamento prioritário.

É importante ressaltar que a primeira Matriz de Risco apresentada na Figura 19 ainda é matriz de riscos que não levou em consideração os efeitos dos controles nos eventos de riscos identificados, posteriormente será apresentada a outra matriz com esses controles considerados.

Outro dado importante é que para a maior relevância de tratamento dos resultados, somente sofreram a identificação dos fatores e efeitos de risco, os fatores de riscos que receberam mais de 5 indicações conforme a Figura 14 desta dissertação.

Figura 19 - Matriz de Riscos.

Impacto						
	Muito Alto 10		ER2-20	ER3-50 ER9-50 ER14-50 ER16-50	ER8-80	
	Alto 8			ER1-40 ER7-40 ER11-40 ER-15-40 ER17-40	ER10-64 ER13-64	
	Moderado 5			ER4-25 ER12-25		
	Pequeno 2			ER6-10		
	Insignificante 1					
		Raro 1	Improvável 2	Possível 5	Provável 8	Muito Alto 10
		Probabilidade				

Risco Baixo Risco Médio Risco Alto Risco Extremo

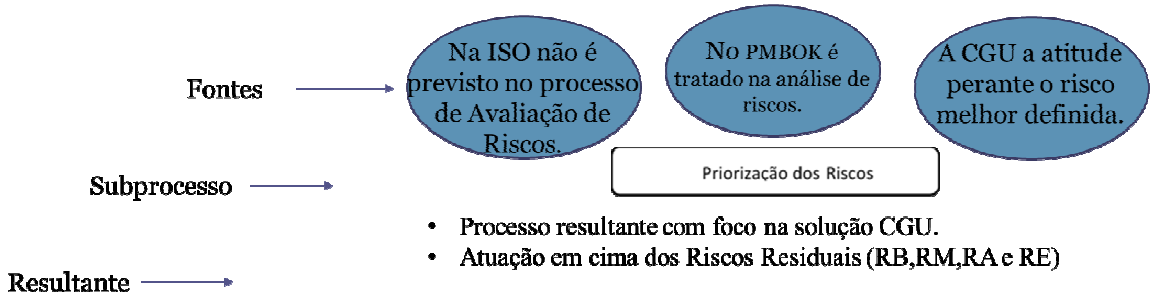
Fonte: Extraída dos resultados da pesquisa de campo, 2020.

4.4. Proposição do Subprocesso de Priorização dos Riscos

O subprocesso de Priorização dos Riscos iniciará tomando por base a fase final de avaliação de riscos da Metodologia de Gestão Riscos da CGU (2018), onde é realizada uma avaliação e é verificado se os controles, quando existentes, são eficazes.

Na Figura 20 são apresentadas as fontes do subprocesso de Priorização de Riscos, onde não é previsto na ISO (2018), no PMBOK (2017) é tratado na Análise dos Riscos e para esse subprocesso iremos usar o que preconiza a CGU (2018).

Figura 20 - Fontes x resultante do subprocesso de Priorização dos Riscos.



Fonte: Elaborada pelo autor, 2019 autor.

Neste subprocesso a entrada é oriunda do subprocesso de Análise e Avaliação do Riscos que é T07-Classificar os Riscos, onde é recebido os riscos classificados e iniciado o subprocesso de Priorização dos Riscos.

Nesta etapa serão testados se os controles preventivos e reativos identificados no subprocesso de Identificação de Riscos auxiliam no tratamento do risco apontado.

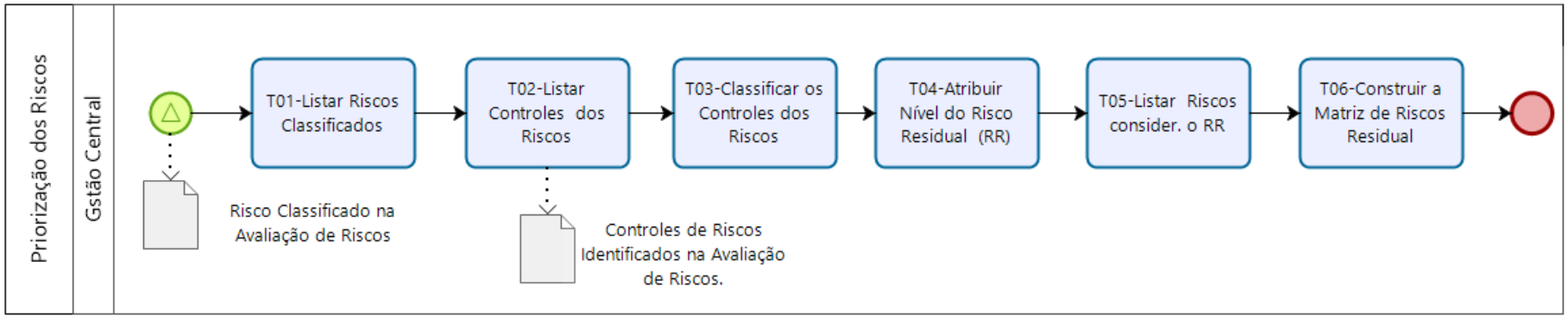
Neste subprocesso são levantados os riscos que devem ser priorizados, segundo a etapa de Priorização dos Riscos da Metodologia de Gestão de Riscos da CGU (2018), a atitude perante o risco deve ser tomada em função dos níveis de Riscos Residuais (RR).

Os Riscos Residuais são resultados do produto entre o valor do Risco Inerente (RI), os encontrados após a classificação dos riscos no subprocesso de Análise e Avaliação de Riscos, e o Fator de Avaliação dos Controles (FC) apontado na Tabela 4.

Em função da classificação do Risco Residual, que pode alterar a classificação do risco, deve-se reavaliar em qual nível de risco se enquadra o Risco Residual.

A Figura 21 apresenta o subprocesso de Priorização dos Riscos e suas atividades sequenciadas.

Figura 21 - Definição do subprocesso Priorização dos Riscos.



Fonte: Elaborada pelo autor (*BPMNotation*), 2020.

Onde,

T01-Listar Riscos Classificados: é a atividade onde são recebidos os Risco Classificado no subprocesso de Avaliação de Riscos.

T02-Listar Controles dos Riscos: é a atividade onde são listados os controles de riscos identificados no subprocesso de Avaliação de Riscos.

T03-Classificar os Controles de Risco: é a atividade onde são avaliados os controles de risco identificados no subprocesso de Identificação de Riscos conforme preconiza o normativo da Metodologia de Gestão de Riscos CGU (2018).

T04-Atribuir Nível do Risco Residual: é a atividade onde o nível de risco recebe o fator dado ao controle de risco e o efeito de risco recebe um novo nível de risco, o Risco Residual.

T05-Listar Riscos Considerando RR: é a atividade onde é listado o nível do evento de risco considerando o Risco Residual.

T06-Listar as Probabilidades Identificadas: é a atividade que recebe as probabilidades aos riscos levantados pelos respondentes e identifica em uma lista as probabilidades para cada risco identificado.

T07-Classificar os Riscos: é a atividade onde a gestão central classifica os riscos em Risco Extremo, Risco Alto, Risco Médio e Risco Baixo em função do produto da probabilidade de ocorrência e o impacto dos riscos identificados.

T08-Construir a Matriz de Risco Residual: é a atividade onde a gestão central constrói a Matriz de Riscos Residual em função dos níveis riscos classificados na atividade anterior, nesta pesquisa foi realizada pelo pesquisador.

4.4.1. Aplicando Dados ao Subprocesso de Priorização dos Riscos

4.4.1.1. Classificação dos Controles de Risco e Aplicação dos Fatores de Avaliação de Risco

Inicialmente são avaliados os controles e são atribuídos os Fatores de Avaliação dos Controles em função do nível do controle que são apresentados na Tabela 4, que podem ser: Inexistente; Fraco; Mediano; Satisfatório e Forte.

Atribuídos os fatores, conforme a Tabela 4, estes são multiplicados pelos valores que foram usados na Matriz de Risco da Figura 19 e do Quadro 6, valores estes sem a aplicação do controle, resultando então nos valores da última coluna, Classificação COM Controle, do Quadro 11.

Quadro 11 - Valores do produto da probabilidade X impacto COM e SEM controle e sua classificação.

				Valores Produto Prob x Imp		
	Eventos de Risco	Controles	Fator	Valores SEM controle	Valores COM controle	Classificação PÓS Controle
ER-1	A rede não suportar o tráfego de novos usuários da Polícia Federal.	Inexistente	1	40	40	RA
ER-2	As informações serem perdidas.	Fraco	0,8	20	16	RM
ER-3	As informações perderem o sigilo.	Inexistente	1	50	50	RA
ER-4	A não adaptação aos equipamentos de outra organização.	Inexistente	1	25	25	RM
ER-6	Os servidores se negarem a usar os equipamentos de outra organização.	Inexistente	1	10	10	RM
ER-7	A Polícia Federal não adquirir os equipamentos/acessórios necessários.	Inexistente	1	40	40	RA
ER-8	A cobertura da nova rede não atender a necessidade de cobertura da Polícia Federal.	Inexistente	1	80	80	RE
ER-9	A Polícia Federal não possuir prioridade da rede em situações de congestionamento.	Fraco	0,8	50	40	RA
ER-10	A nova rede não disponibilizar o modo tático para operações onde não haja cobertura.	mediano	0,6	64	38,4	RM
ER-11	O Convênio de compartilhamento ser desfeito sem a devida programação.	mediano	0,6	40	24	RM
ER-12	A gerência da rede está em outra organização.	Inexistente	1	25	25	RM
ER-13	A falta de autonomia para alterar parâmetros que melhor atendem a Polícia Federal.	Fraco	0,8	64	51,2	RA
ER-14	A não possibilidade de escolha dos fornecedores.	Fraco	0,8	50	40	RA
ER-15	A não possibilidade de fazer uso de criptografia própria.	Fraco	0,8	40	32	RM
ER-16	A vulnerabilidade de acesso aos centros de controle de outras organizações.	Fraco	0,8	50	40	RA
ER-17	Desconhecimento do pessoal que acessa os centros de controle de outras organizações.	Fraco	0,8	40	32	RM

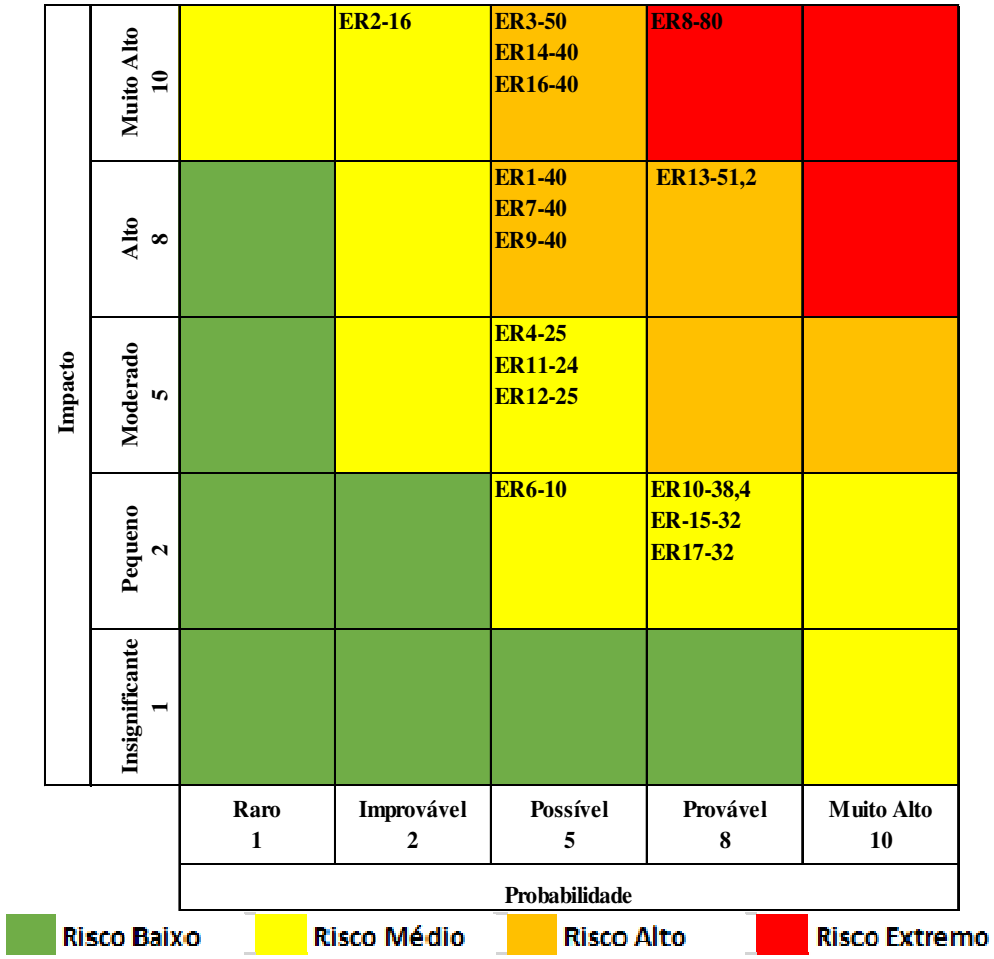
Risco Baixo Risco Médio Risco Alto Risco Extremo

Fonte: Extraído dos resultados da pesquisa, 2020.

4.4.1.2. Construir a Matriz de Riscos COM controles aplicados

O próximo passo é aplicação dos valores encontrados para classificação dos riscos com o efeito dos controles na Matriz de Risco. É apresentada a nova Matriz de Riscos por meio da Figura 22.

Figura 22 - Matriz de Riscos COM controles aplicados.



Fonte: Extraída dos resultados da pesquisa, 2020.

A Matriz de Riscos apresentada possui os controles aplicados, os níveis de risco são alterados em relação a matriz anterior, a Matriz de Riscos sem os controles aplicados, em função desta nova matriz apresentar os níveis de risco com os controles reativos e preventivos aplicados aos eventos de risco.

4.4.1.3. Comparação entre as Matrizes de Risco com e sem os Controles Aplicados

Na Figura 23 são apresentadas as duas Matrizes de Risco, a primeira sem os controles aplicados aos eventos de risco e a segunda com os controles aplicados aos eventos de risco.

Figura 23 - Comparação entre as Matrizes de Risco SEM e COM controles

Matriz de Riscos SEM os controles aplicados

Impacto		Raro 1	Improvável 2	Possível 5	Provável 8	Muito Alto 10
	Muito Alto 10		ER2-20	ER3-50 ER9-50 ER14-50 ER16-50	ER8-80	
	Alto 8			ER1-40 ER7-40 ER11-40 ER-15-40 ER17-40	ER10-64 ER13-64	
	Moderado 5			ER4-25 ER12-25		
	Pequeno 2			ER6-10		
	Insignificante 1					
		Probabilidade				

X

Matriz de Riscos COM os controles aplicados

Impacto		Raro 1	Improvável 2	Possível 5	Provável 8	Muito Alto 10
	Muito Alto 10		ER2-16	ER3-50 ER14-40 ER16-40	ER8-80	
	Alto 8			ER1-40 ER7-40 ER9-40	ER13-51,2	
	Moderado 5			ER4-25 ER11-24 ER12-25		
	Pequeno 2			ER6-10	ER10-38,4 ER-15-32 ER17-32	
	Insignificante 1					
		Probabilidade				

Risco Baixo | Risco Médio | Risco Alto | Risco Extremo

Fonte: Extraída dos resultados da pesquisa, 2020.

É possível perceber que a classificação dos níveis de risco sofrera pouca alteração em relação aos valores de níveis encontrados para a matriz de riscos sem controle, isso ocorreu porque a maioria dos controles encontrados foram inexistentes ou fracos, o que pouco contribui para alterar o nível de risco encontrado anteriormente sem o controle aplicado.

Essa pouca alteração em relação aos níveis de riscos quando são comparados os níveis de risco com e sem os controles aplicados, demostra a baixa maturidade do processo de avaliação de risco ao se compartilhar sistemas de radiocomunicações na organização em estudo, com o passar do tempo associado a maturidade do processo de avaliação de riscos, a organização tente a tornar os seus controles mais eficazes, o que elevaria os fatores dos controles de risco, contribuindo para diminuir o nível de risco dos eventos identificados ao compartilhar sistemas de radiocomunicações.

5. VALIDAÇÃO DOS RESULTADOS DO *FRAMEWORK*

5.1. Validação de Especialistas

A etapa da Validação foi realizada por especialistas, apenas três participaram desta etapa, servidores com larga experiencia na área de radiocomunicação na organização.

Inicialmente foi apresentada a pesquisa, todos os participantes tinham conhecimento da pesquisa por terem participado da 1ª etapa da pesquisa de campo, onde foram levantados os eventos de risco, as probabilidades de ocorrência e o impacto da ocorrência destes eventos de risco na organização, no entanto, por meio desta etapa de validação, ao apresentar a pesquisa, se apresentou uma oportunidade para apresentar a pesquisa e seus objetivos de uma forma mais aprofundada.

Foram apresentados os resultados da pesquisa, os eventos de riscos identificados, as tabelas com as indicações pelos pesquisados, as probabilidades e os impactos selecionados pelos pesquisados, o Quadro 7 com os Fatores de Risco, os Efeitos de Risco e os Controles Preventivos e Reativos, o Quadro 11 com os níveis dos controles internos levantados na pesquisa para a definição dos fatores de avaliação dos riscos identificados e a Matriz de Riscos da Figura 22.

5.2. Validação dos Fatores e Efeitos de Risco e seus controles

Para a próxima etapa, a validação dos Fatores e Efeitos de Risco e seus controles, os preventivos e os reativos, foi apresentado o Quadro 7.

Ao apresentar o Quadro 7 aos especialistas, obtivemos as seguintes respostas demonstradas no Quadro 12 para a validação dos itens, onde a observação são as contribuições dos respondentes para cada item.

Quadro 12 - Respostas da avaliação dos especialistas quanto aos resultados do Quadro 4.

			Discordo Totalmente	Discordo	Não estou decidido	Concordo	Concordo Totalmente	Observações
Evento de Risco 1	Fatores		0	0	0	1	2	
	Efeitos		0	0	0	2	1	
	Controle	Preventivo	0	0	0	0	3	
		Reativos	0	0	0	1	2	
Evento de Risco 2	Fatores		0	0	0	0	3	
	Efeitos		0	0	0	1	2	
	Controle	Preventivo	0	0	0	0	3	
		Reativos	0	0	0	1	2	Colocar o sistema anterior para funcionar.
Evento de Risco 3	Fatores		0	0	0	0	3	
	Efeitos		0	0	0	2	1	
	Controle	Preventivo	0	0	0	0	3	
		Reativos	0	0	0	1	2	
Evento de Risco 4	Fatores		0	0	0	0	3	
	Efeitos		0	0	0	1	2	
	Controle	Preventivo	0	0	0	0	3	
		Reativos	0	0	0	2	1	
Evento de Risco 6	Fatores		0	0	0	1	2	
	Efeitos		0	0	0	2	1	As operações ficarem sem comunicação.
	Controle	Preventivo	0	0	0	1	2	
		Reativos	0	0	0	2	1	Baixar normativos que obriguem os servidores a usar.

Evento de Risco 7	Fatores		0	0	0	1	2	
	Efeitos		0	0	0	0	3	
	Controle	Preventivo	0	0	0	0	3	
		Reativos	0	0	0	0	3	
Evento de Risco 8	Fatores		0	0	0	0	3	
	Efeitos		0	0	0	1	2	
	Controle	Preventivo	0	0	0	0	3	
		Reativos	0	0	0	0	3	
Evento de Risco 9	Fatores		0	0	0	0	3	
	Efeitos		0	0	0	1	2	
	Controle	Preventivo	0	0	0	1	2	
		Reativos	0	0	0	1	2	
Evento de Risco 10	Fatores		0	0	0	1	2	
	Efeitos		0	0	0	2	1	
	Controle	Preventivo	0	0	0	0	3	Manter o Sistema Atual Tático.
		Reativos	0	0	0	1	2	
Evento de Risco 11	Fatores		0	0	0	0	3	
	Efeitos		0	0	0	1	2	
	Controle	Preventivo	0	0	0	0	3	
		Reativos	0	0	0	1	2	
Evento de Risco 12	Fatores		0	0	0	1	2	O sistema ter sido comprado por outro órgão.
	Efeitos		0	0	0	2	1	
	Controle	Preventivo	0	0	0	0	3	
		Reativos	0	0	0	1	2	

Evento de Risco 13	Fatores		0	0	0	1	2	
	Efeitos		0	0	0	2	1	
	Controle	Preventivo	0	0	0	0	3	
		Reativos	0	0	0	1	2	
Evento de Risco 14	Fatores		0	0	0	1	2	
	Efeitos		0	0	0	2	1	
	Controle	Preventivo	0	0	0	0	3	
		Reativos	0	0	0	0	3	
Evento de Risco 15	Fatores		0	0	0	0	3	
	Efeitos		0	0	0	1	2	As comunicações perderem o sigilo.
	Controle	Preventivo	0	0	0	0	3	
		Reativos	0	0	0	0	3	
Evento de Risco 16	Fatores		0	0	0	0	3	
	Efeitos		0	0	0	1	2	
	Controle	Preventivo	0	0	0	0	3	
		Reativos	0	0	0	2	1	
Evento de Risco 17	Fatores		0	0	0	2	1	
	Efeitos		0	0	0	2	1	As comunicações perderem o sigilo.
	Controle	Preventivo	0	0	0	0	3	
		Reativos	0	0	1	1	1	

Fonte: Extraído dos resultados da pesquisa, 2020.

É possível observar nas respostas dos especialistas, que estes concordam com grande maioria dos fatores de riscos, efeitos de riscos, controles preventivos e controles reativos, e ainda foram realizadas contribuições, que estão destacadas e circuladas em vermelho, que levaram a adicionar informações no Quadro 7 que é apresentado abaixo como Quadro 13.

Quadro 13 - Identificação dos fatores e efeito de risco e seus controles com contribuição dos especialistas que participaram da validação.

Evento de Risco 1 - A rede não suportar o tráfego de novos usuários da Polícia Federal.			
Fatores	Poucos canais disponíveis. Muitos usuários usando a rede numa mesma região. A rede não foi planejada para ser compartilhada. Falta de manutenção da rede.	Preventivo	Instalar maior número de canais. Planejar a comunicação de operações integradas. Prever maior número de canais quando da entrada de novos parceiros na rede. Criar o ciclo de manutenção preventiva do sistema.
Efeito	Equipes incomunicáveis. Congestionamento da rede.	Reativo	Elaborar comunicação de contingência. Coordenar o fluxo prioritário de comunicação da rede.
Evento de Risco 2 - As informações serem perdidas.			
Fatores	Inoperância a rede. Perda de backup das informações. O não acesso ao core da rede.	Preventivo	Elaborar comunicação de contingência. Criação de rotinas de backups. Negociar o compartilhamento do core da rede.
Efeito	Falta de informações de uso da rede pelos usuários. Atraso nas respostas das demandas dos usuários.	Reativo	Colocar o sistema anterior para funcionar. Busca acesso aos backups. Busca de dados em local fora de sistemas.
Evento de Risco 3 - As informações perderem o sigilo.			
Fatores	Acesso não autorizado nas bases do sistema. Uso de equipamentos de rádio não autorizado. Escuta não autorizado de informações da organização. Quebra da criptografia.	Preventivo	Identificação dos acessos e trocas de senhas periódicas. Possuir controle de uso de rádios dos usuários. Buscar protocolos de restrição de acesso aos dados da organização. Atualização das criptografias do sistema.

Efeito	Acesso não autorizado das informações da organização.	Reativo	Uso de códigos nas comunicações que dificultem o entendimento das informações trafegadas.
Evento de Risco 4 - A não adaptação aos equipamentos de outra organização.			
Fatores	Equipamentos diferentes dos usualmente usados. Falta de treinamento nos novos equipamentos. Falta de acessórios úteis a missão da organização. Equipamentos não adaptados a missão da organização.	Preventivo	Realizar treinamento nos novos equipamentos. Realizar treinamento nos novos equipamentos. Buscar os acessórios necessários ao cumprimento à missão da organização. Buscar equipamentos na nova rede que atendam as particularidades da organização.
Efeito	Os servidores não usarem os novos equipamentos. Busca de um sistema que atenda das necessidades da organização.	Reativo	Campanhas de uso e importância do da comunicação numa organização de segurança. Continuar prospectando sistema de comunicação próprio.
Evento de Risco 6 - Os servidores se negarem a usar os equipamentos por serem equipamentos de outra organização.			
Fatores	Não adaptação aos equipamentos. Falta de treinamento. Rejeição ao uso de novos equipamentos.	Preventivo	Campanhas de uso e importância do da comunicação numa organização de segurança. Realizar treinamentos de uso dos equipamentos. Campanhas de uso e importância do da comunicação numa organização de segurança.
Efeito	As operações ficarem sem comunicação.funcionar. Os servidores não usarem os novos equipamentos.	Reativo	Baixar normativos que obriguem os servidores a usar. Realizar treinamento nos novos equipamentos.
Evento de Risco 7 - A Polícia Federal não adquirir os equipamentos/acessórios necessários para o uso da nova rede.			
Fatores	Falta de recursos para compra dos equipamentos / acessórios. Não serem disponibilizados pelo fornecedor equipamentos / acessórios de acordo com a particularidade da organização.	Preventivo	Buscar orçamento justificando a necessidade do recurso para compra dos equipamentos/acessórios que atendam a necessidade da organização. Buscar com outros fornecedores equipamentos / acessórios que atendam a necessidade da organização.

Efeito	Os servidores não usarem os novos equipamentos.	Reativo	Campanhas de uso e importância do da comunicação numa organização de segurança até que se busque os equipamentos/acessórios que atendam a necessidade da organização.
Evento de Risco 8 - A cobertura da nova rede não atender a necessidade de cobertura da Polícia Federal.			
Fatores	Falhas de estações. Não previsão dos locais que interessam a organização nos projetos de instalação.	Preventivo	Buscar orçamento justificando a necessidade do recurso para compra dos equipamentos / acessórios que atendam a necessidade da organização. Buscar com outros fornecedores de equipamentos / acessórios que atendam a necessidade da organização.
Efeito	Falta de cobertura nos locais de atuação da organização. Os servidores não usarem os novos equipamentos.	Reativo	Buscar junto ao gestor da rede a instalação de novas estações de transmissão que atendam a organização. Campanhas de uso e importância do da comunicação numa organização de segurança até que se obtenha coberturas que atendam a necessidade da organização.
Evento de Risco 9 - A Polícia Federal não possuir prioridade da rede em situações de congestionamento.			
Fatores	A não previsão de prioridade da rede no projeto de instalação do sistema. Falta de disponibilidade de canais de comunicação.	Preventivo	Solicitar junto ao gestor da rede a prioridade dos canais. Aumento do número de canais da rede.
Efeito	Os servidores não conseguirem usar a rede de comunicação.	Reativo	Busca de um sistema de comunicação de contingencias.
Evento de Risco 10 - A nova rede não disponibilizar o modo tático para operações onde não haja cobertura			
Fatores	O sistema não disponibilizar sistema tático. A Polícia Federal não adquirir o sistema tático.	Preventivo	Manter o Sistema Atual Tático. Buscar um sistema de contingencias que supra o modo tático Realizar estudos para a compra do sistema tático.
Efeito	Falta de cobertura em áreas remotas.	Reativo	Busca de um sistema de contingencias para suprir o modo tático.

Evento de Risco 11 - O Convênio de compartilhamento ser desfeito sem a devida programação.			
Fatores	Falta de gerencia dos prazos do contrato. Descumprimento dos acordos do contrato. Não atendimento das necessidades de comunicação da organização.	Preventivo	Manter os cuidados com os prazos e gerencia dos prazos junto a organização parte do contrato. Manter os cuidados para o cumprimento dos acordos contratuais da organização previstos no contrato. Buscar sistemas de contingencias e prospectar sistemas próprios de comunicação.
Efeito	Os servidores não conseguirem usar a rede de comunicação.	Reativo	Busca de um sistema de comunicação de contingencias.
Evento de Risco 12 - A gerência da rede está em outra organização.			
Fatores	O sistema ter sido comprado por outro orgão. A organização ser a detentora da gerência da rede. O sistema não permitir espelhamento da gerencia da rede.	Preventivo	Buscar junto à organização que gerencia a rede acesso aos controles da rede. Buscar junto à organização o espelhamento da gerencia do sistema.
Efeito	Não ser possível customizar a rede como as alterações que melhor atendem a organização.	Reativo	Buscar junto à organização que possui a gerencia da rede as possibilidades de customizar a rede para que melhor possa atender a Polícia Federal.
Evento de Risco 13 - A falta de autonomia para alterar parâmetros que melhor atendem a Polícia Federal.			
Fatores	A organização ser a detentora da gerência da rede. Não ser previsto em contrato a autonomia necessária para alterações de parâmetros que melhor atendem a Polícia Federal.	Preventivo	Buscar junto à organização que gerencia a rede acesso aos controles da rede. Buscar instruir cláusulas no contrato de compartilhamento que permitam a Polícia Federal alterar parâmetros que melhor lhe atendam.
Efeito	Não ser possível customizar a rede como as alterações que melhor atendem a organização. Os servidores não conseguirem usar a rede de comunicação.	Reativo	Buscar junto à organização que possui a gerencia da rede as possibilidades de customizar a rede para que melhor possa atender a Polícia Federal. Busca de um sistema de comunicação de contingencias.
Evento de Risco 14 - A não possibilidade de escolha dos fornecedores. Já que os fornecedores já atendem a outra organização.			
Fatores	O contrato pertencer a outra organização.	Preventiv	Busca aproximação aos fornecedores para atender as necessidades da PF. Prospectar uma rede de radiocomunicação

	A Polícia Federal não possuir interesse em ter uma rede própria.		própria.
Efeito	Fornecedores com propostas engessadas de preço e disponibilidade de material diferenciado.	Reativo	Prover gestões junto aos fornecedores materiais que atenda a organização com preços de mercado.
Evento de Risco 15 - A não possibilidade de fazer uso de criptografia própria.			
Fatores	A criptografia já vier inserida no sistema contratado. O gerador de chaves criptográficas não ficar instalado na Polícia Federal. O sistema não possibilitar instalar criptografia própria.	Preventivo	Buscar junto à organização que gerencia o sistema a possibilidade de instalar uma criptografia própria da Polícia Federal. Buscar junto à organização que gerencia o sistema instalar na Polícia Federal o gerador de chaves criptográficas. Buscar junto aos fornecedores e ao gestor do sistema de comunicações os meios para instalar uma criptografia própria.
Efeito	As comunicações perderem o sigilo. A Polícia Federal fazer uso de uma criptografia comum na organização. Os servidores não usarem os novos equipamentos.	Reativo	Fazer uso de controle controles de segurança próprios dos equipamentos que possibilitem a customização para a atividade da Polícia Federal. Buscar de novos equipamentos que atendam a organização.
Evento de Risco 16 - A vulnerabilidade de acesso aos centros de controle de outras organizações.			
Fatores	Os centros de controle estar em outra organização. Desconhecimento dos controles aplicados pela organização que gerencia o sistema.	Preventivo	Buscar informações e combinar protocolos de acesso com a outra organização. Buscar informações e participar dos controles que existem nos centros de controle.
Efeito	As informações trafegadas pela organização estarem expostas.	Reativo	Procurar fazer uso de códigos na comunicação.
Evento de Risco 17 - Desconhecimento do pessoal que acessa os centros de controle de outras organizações.			
Fatores	Não participar da seleção de pessoas que acessam o sistema. A gestão do centro de controle não estar na Polícia Federal.	Preventivo	Buscar informações das pessoas que acessam os centros de controle. Buscar informações das pessoas que acessam os centros de controle.

Efeito	As comunicações perderem o sigilo. As informações trafegadas pela organização estarem expostas.	Reativo	Procurar fazer uso de códigos na comunicação.

Fonte: Elaborado pelo autor, 2020.

Essa concordância pelos especialistas ratifica os resultados alcançados, somente para o Evento de Risco 17 se obteve uma resposta onde o especialista não estaria decidido sobre os controles reativos, mas como um concorda totalmente, e outro concorda, foi considerado como válido o controle apresentado para este evento de risco.

5.3. Validação dos Controles dos Fatores de Riscos

A etapa seguinte foi apresentar o Quadro 11, onde se procurou validar os níveis dos controles internos levantados na pesquisa para a definição dos fatores de avaliação dos riscos identificados.

Nesta etapa da validação os respondentes especialistas avaliaram para cada controle dos Fatores de Riscos identificados, se concordavam com o controle aplicado e no caso de não concordarem, qual a avaliação para esse especialista do controle estudado.

No Quadro 14, é apresentado a avaliação dos especialistas aos controles e o resultado desta avaliação, onde para a coluna “Resultado” foi considerado a moda dos resultados. Para os casos em que existiram o empate dentre os mais escolhidos, foi considerado a maior quantidade de vezes selecionada pelos especialistas.

Quadro 14 - Avaliação dos especialistas quanto aos controles dos fatores de riscos identificados.

			Especialistas			
	Eventos de Risco	Controles	1	2	3	Resultado
ER-1	A rede não suportar o tráfego de novos usuários da Polícia Federal.	Inexistente	Inexistente	Fraco	Inexistente	Inexistente
ER-2	As informações serem perdidas.	Fraco	Fraco	Inexistente	Inexistente	Inexistente
ER-3	As informações perderem o sigilo.	Inexistente	Inexistente	Inexistente	Fraco	Inexistente
ER-4	A não adaptação aos equipamentos de outra organização.	Inexistente	Inexistente	Inexistente	Fraco	Inexistente
ER-6	Os servidores se negarem a usar os equipamentos de outra organização.	Inexistente	Inexistente	Inexistente	Inexistente	Inexistente
ER-7	A Polícia Federal não adquirir os equipamentos/acessórios necessários.	Inexistente	Inexistente	Fraco	Inexistente	Inexistente
ER-8	A cobertura da nova rede não atender a necessidade de cobertura da Polícia Federal.	Inexistente	Inexistente	Inexistente	Inexistente	Inexistente
ER-9	A Polícia Federal não possuir prioridade da rede em situações de congestionamento.	Fraco	Inexistente	mediano	Inexistente	Inexistente
ER-10	A nova rede não disponibilizar o modo tático para operações onde não haja cobertura.	mediano	Fraco	Inexistente	Fraco	Fraco
ER-11	O Convênio de compartilhamento ser desfeito sem a devida programação.	mediano	mediano	Fraco	Inexistente	mediano
ER-12	A gerência da rede está em outra organização.	Inexistente	Fraco	Fraco	Inexistente	Fraco
ER-13	A falta de autonomia para alterar parâmetros que melhor atendem a Polícia Federal.	Fraco	Inexistente	Inexistente	Fraco	Inexistente
ER-14	A não possibilidade de escolha dos fornecedores.	Fraco	Fraco	Fraco	Inexistente	Fraco
ER-15	A não possibilidade de fazer uso de criptografia própria.	Fraco	mediano	Fraco	Inexistente	Fraco
ER-16	A vulnerabilidade de acesso aos centros de controle de outras organizações.	Fraco	Fraco	Inexistente	Inexistente	Inexistente
ER-17	Desconhecimento do pessoal que acessa os centros de controle de outras organizações.	Fraco	Inexistente	Inexistente	Fraco	Inexistente

Fonte: Extraído dos resultados da pesquisa, 2020.

O passo seguinte foi atribuir o Fator de Avaliação dos Controles em função dos resultados obtidos com a participação dos especialistas na validação, em função destes, foram definidos os valores de probabilidade x impacto a serem usados na atribuição dos níveis de riscos a serem usados na Matriz de Riscos., valores estes demostrados no Quadro 15 na coluna “Classificação COM Controle”.

Quadro 15 - Valores do produto da probabilidade X impacto COM controle e sua classificação atribuídos na validação pelos especialistas.

				Valores Produto Prob x Imp			
	Eventos de Risco	Resultado	Fator	Valores SEM controle	Valores COM controle ANTES Validação	Valores COM controle APÓS Validação	Classificação PÓS Validação
ER-1	A rede não suportar o tráfego de novos usuários da Polícia Federal.	Inexistente	1	40	40	40	RA
ER-2	As informações serem perdidas.	Inexistente	1	20	16	20	RM
ER-3	As informações perderem o sigilo.	Inexistente	1	50	50	50	RA
ER-4	A não adaptação aos equipamentos de outra organização.	Inexistente	1	25	25	25	RM
ER-6	Os servidores se negarem a usar os equipamentos de outra organização.	Inexistente	1	10	10	10	RM
ER-7	A Polícia Federal não adquirir os equipamentos/acessórios necessários.	Inexistente	1	40	40	40	RA
ER-8	A cobertura da nova rede não atender a necessidade de cobertura da Polícia Federal.	Inexistente	1	80	80	80	RE
ER-9	A Polícia Federal não possuir prioridade da rede em situações de congestionamento.	Inexistente	1	50	40	50	RA
ER-10	A nova rede não disponibilizar o modo tático para operações onde não haja cobertura.	Fraco	0,8	64	38,4	51,2	RA
ER-11	O Convênio de compartilhamento ser desfeito sem a devida programação.	mediano	0,6	40	24	24	RM
ER-12	A gerência da rede está em outra organização.	Fraco	0,8	25	25	20	RM
ER-13	A falta de autonomia para alterar parâmetros que melhor atendem a Polícia Federal.	Inexistente	1	64	51,2	64	RA
ER-14	A não possibilidade de escolha dos fornecedores.	Fraco	0,8	50	40	40	RA
ER-15	A não possibilidade de fazer uso de criptografia própria.	Fraco	0,8	40	32	32	RM
ER-16	A vulnerabilidade de acesso aos centros de controle de outras organizações.	Inexistente	1	50	40	50	RA
ER-17	Desconhecimento do pessoal que acessa os centros de controle de outras organizações.	Inexistente	1	40	32	40	RA

Risco Baixo | Risco Médio | Risco Alto | Risco Extremo

Fonte: Extraído dos resultados da pesquisa, 2020.

5.4. Elaboração da Matriz de Risco após Validação

O último passo da validação foi a elaboração da nova Matriz de Riscos com os níveis identificados após a validação dos especialistas, esta Matriz de Riscos é apresentada na Figura 24.

Figura 24 - Comparação entre as Matrizes de Risco ANTES e APÓS a Validação.

Matriz de Risco – COM controle – ANTES Especialistas

Impacto	Raro 1	Improvável 2	Possível 5	Provável 8	Muito Alto 10
Muito Alto 10		ER2-16	ER3-50 ER14-40 ER16-40	ER8-80	
Alto 8			ER1-40 ER7-40 ER9-40	ER13-51,2	
Moderado 5			ER4-25 ER11-24 ER12-25		
Pequeno 2			ER6-10	ER10-38,4 ER-15-32 ER17-32	
Insignificante 1					

Probabilidade

Matriz de Risco – COM controle – APÓS Especialistas

Impacto	Raro 1	Improvável 2	Possível 5	Provável 8	Muito Alto 10
Muito Alto 10		ER2-20	ER3-50 ER14-40 ER16-50	ER8-80	
Alto 8			ER1-40 ER7-40 ER9-50	ER13-64	
Moderado 5			ER4-25 ER11-24 ER12-20	ER10-51,2	ER17-40
Pequeno 2			ER6-10	ER-15-32	
Insignificante 1					

Probabilidade

Risco Baixo | Risco Médio | Risco Alto | Risco Extremo

Fonte: Extraída dos resultados da pesquisa, 2020.

Observando a Figura 24 foi possível perceber a mudança dos seguintes Eventos de Risco:

O Evento de Risco 2 teve alterado o resultado do produto da Probabilidade x Impacto de 16 para 20. Essa alteração se deu em função da alteração dos níveis de avaliação dos controles existentes, no entanto, foi possível observar a não alteração do nível de riscos atribuído ao evento de risco estudado, mantendo-se em risco médio (RM) considerando a Tabela 3 deste estudo;

O Evento de Risco 9 teve alterado o resultado do produto da Probabilidade x Impacto de 40 para 50. Essa alteração se deu em função da alteração dos níveis de avaliação dos controles existentes, no entanto, foi possível observar a não alteração do nível de riscos atribuído ao evento de risco estudado, mantendo-se em risco alto (RA) considerando a Tabela 3 deste estudo;

O Evento de Risco 10 teve alterado o resultado do produto da Probabilidade x Impacto de 38,4 para 51,2. Essa alteração se deu em função da alteração dos níveis de avaliação dos controles existentes, para este evento de risco foi possível observar a alteração do nível de riscos atribuído ao evento de risco estudado, este foi alterado de risco médio (RM) para risco alto (RA) considerando a Tabela 3 deste estudo;

O Evento de Risco 12 teve alterado o resultado do produto da Probabilidade x Impacto de 25 para 20. Essa alteração se deu em função da alteração dos níveis de avaliação dos controles existentes, no entanto, foi possível observar a não alteração do nível de riscos atribuído ao evento de risco estudado, mantendo-se em risco médio (RM) considerando a Tabela 3 deste estudo;

O Evento de Risco 13 teve alterado o resultado do produto da Probabilidade x Impacto de 51,2 para 64. Essa alteração se deu em função da alteração dos níveis de avaliação dos controles existentes, no entanto, foi possível observar a não alteração do nível de riscos atribuído ao evento de risco estudado, mantendo-se em risco alto (RA) considerando a Tabela 3 deste estudo;

O Evento de Risco 16 teve alterado o resultado do produto da Probabilidade x Impacto de 40 para 50. Essa alteração se deu em função da alteração dos níveis de avaliação dos controles existentes, no entanto, foi possível observar a não alteração do nível de riscos atribuído ao evento de risco estudado, mantendo-se em risco alto (RA) considerando a Tabela 3 deste estudo;

O Evento de Risco 17 teve alterado o resultado do produto da Probabilidade x Impacto de 32 para 40. Essa alteração se deu em função da alteração dos níveis de avaliação

dos controles existentes, para este evento de risco foi possível observar a alteração do nível de riscos atribuído ao evento de risco estudado, este foi alterado de risco médio (RM) para risco alto (RA) considerando a Tabela 3 deste estudo;

É possível concluir que existiram alterações nos resultados do produto de impacto x probabilidade de alguns eventos de risco, dos 16 Eventos de Risco avaliados pelos especialistas na etapa de validação, existiram 7 Eventos de Risco (ER2, ER9, ER10, ER12, ER13, ER16 e ER17) que sofreram alterações do valor da Probabilidade x Impacto, no entanto, 5 destas alterações não foram suficientes para alterar os níveis de risco, mantendo então os níveis anteriores, porém, existiram 2 Eventos de Risco (ER10 e ER17) que além de sofrerem alterações nos seus valores Probabilidade x Impacto, sofreram também alteração da classificação dos seus níveis de riscos, ambas passando de níveis de risco médio (RM) para risco alto (RA).

5.5. Conclusões da Validação

A validação teve um papel importante, pois servidores com maior experiência ao participarem da validação ratificam e ajustaram os resultados obtidos na pesquisa e acrescentaram sugestões de melhorias nos fatores e efeitos de riscos e nos controles preventivos e reativos identificados.

Os especialistas tiverem uma importante participação no resultado final dos controles atribuídos para a devida classificação dos níveis de avaliação dos controles existentes, a readequação dos níveis em função da contribuição dos especialistas procurou retornar resultados mais próximos da realidade considerando os diferentes contextos e realidades no qual estão inseridos os especialistas e a organização de estudo.

Foi possível observar algumas alterações dos níveis e classificações dos controles com a contribuição dos especialistas, essa alteração direciona as ações e recursos quanto ao tratamento dos eventos de riscos identificados durante a pesquisa, contribuindo dessa forma para que os esforços, sejam eles para mitigar ou eliminar estes riscos, possam ser direcionados para atender aos objetivos da organização, para o caso, o compartilhamento de sistemas de radiocomunicações entre forças de segurança.

6. CONCLUSÕES

Por meio da pesquisa, foi proposto um *Framework* aplicado ao domínio do compartilhamento de sistemas de radiocomunicações, adaptado a partir de modelos de gestão de riscos já estabelecidos. Na pesquisa de campo foram identificados os eventos de risco, seus impactos e as probabilidades de ocorrência destes eventos de risco. Foram identificados suas causas, efeitos e seus controles preventivos e reativos, foi entregue um *dashboard* dos Eventos de Risco associados aos seus níveis de risco por meio de uma Matriz de Riscos que foi resultado do produto das variáveis Probabilidade e o Impacto de ocorrerem os eventos de risco identificados, identificadas na pesquisa de campo.

A aplicação do *Framework* proposto foi validada através das contribuições dos especialistas gestores de sistemas de radiocomunicações dos setores de TI da Polícia Federal. Foram realizadas adequações e ajustados os controles internos da organização para os eventos de riscos identificados para que estes melhores representassem a realidade da organização de estudo, visto que, por meio da matriz de Riscos é possível identificar e definir as prioridades no tratamento dos eventos de riscos em função de sua criticidade.

Foram alcançados resultados, como: a revisão da literatura com organização da fundamentação teórica sobre os normativos de gestão de riscos; as tecnologias que compõem os sistemas de radiocomunicações; o compartilhamento de estruturas; a organização dos macro e subprocessos de diferentes *Frameworks*; a proposição de um processo (*Framework de Análise de Riscos do Compartilhamento de Sistemas de Radiocomunicações entre Forças de Segurança)*, aplicável e replicável; a identificação e categorização de riscos (fatores, eventos e efeitos) do domínio estudado; e envolvimento de terceiros no estudo de campo para posterior aplicação do *Framework* na organização de estudo e nas organizações de segurança.

A aplicação do *Framework* traz diversas vantagens para a organização como: a padronização de um método descrito no passo a passo de como a organização deve realizar o compartilhamento de sistemas de radiocomunicações, método esse que teve a participação de diversos gestores que participaram da pesquisa e identificaram previamente os riscos de se compartilhar sistemas de radiocomunicações; identificação dos fatores de Risco, os Efeitos de Risco e seus controles preventivos e reativos ajustados pela etapa de validação; um *dashboard* dos riscos identificados associados aos níveis de risco o que contribuirá e influenciará as decisões positivas de mitigação e eliminação dos Eventos dos Riscos.

Estes resultados contribuem para facilitar o compartilhamento de sistemas de radiocomunicações entre forças de segurança e auxiliar na elaboração de processos específicos de análise de riscos destes compartilhamentos.

Este estudo limitou-se a não estudar a ortogonalidade de Eventos de Riscos em diferentes Fatores de Risco e seus Efeitos de Risco. As análises deste estudo procuraram retratar a relação de determinado Efeito de Risco com seus próprios fatores e efeitos relacionados ao mesmo Evento de Risco. Não estuda por exemplo, a relação de determinada causa influenciando em diversos Eventos de Risco ou diferentes efeitos relacionados a um mesmo Evento de Risco.

Além desta limitação, pode-se citar também que esse estudo procura se limitar ao compartilhamento entre organizações públicas de segurança ou defesa.

Não foram encontrados trabalhos correlatos, por se tratar de um assunto muito específico, mesmo se tratando de outros estudos de avaliação de riscos entre estruturas, sejam elas governamentais ou de segurança de outra espécie.

Essa pesquisa traz uma importante contribuição para o campo específico em estudo do compartilhamento de sistemas de radiocomunicações, pois muitos investimentos foram realizados em redes de radiocomunicações com vistas aos grandes eventos que ocorreram no Brasil desde o ano de 2007 e diversas dessas redes estão se tornando obsoletas pelos mais diversos fatores. Atualmente diversas organizações planejam os futuros caminhos de suas redes instaladas e um dos prováveis cenários é uma rede única, compartilhada entre forças de segurança, sobre argumentos fortes que são o investimento único e a capacidade de realizar operações integradas entre forças com maior facilidade e eficiência, por estarem todos os órgãos num mesmo centro de controle centralizado.

A análise de riscos desse compartilhamento contribui para que as organizações passem a pisar em solo conhecido, sobre critérios técnicos e práticos, dessa forma contribuindo com a viabilidade do compartilhamento de sistemas de radiocomunicações entre organizações de segurança pública e defesa no Brasil.

Para trabalhos futuros, sugere-se a elaboração de um software para automatização do *Framework* apresentado.

7. REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27005*: Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação. Rio de Janeiro. 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO 31000*: Gestão de Riscos – Princípios e diretrizes. 2018.

AGUIAR, M. Gerenciando riscos nos projetos de software, 2011. Disponível em: <http://www.metricas.com.br/downloads/Gerenciamento_de_Riscos.pdf> Acessado em: 16/05/2020.

ALVIM, P. Tirando o Máximo do Java EE 6 Open Source com jCompany Developer Suite. 3. Ed. Belo Horizonte: Powerlogic Publishing, 2010.

AMARAL, C. T. Rede de Rádio Digital de Segurança Pública: Estudo de Caso para a Copa do Mundo de Futebol em Belo Horizonte. Trabalho de Conclusão de Curso de Especialização, Centro Universitário de Belo Horizonte, 2010.

ASSUMPÇÃO L. E MINGHELLI M.. Aproximação entre a Ciência da Informação com a Ciência Policial. 1 ed. Cap.XIV. Florianópolis, 2019.

BARCELLOS, P. Energia Elétrica, Telecomunicações e Livre Acesso. Correio Braziliense (Caderno Direito e Justiça, p. 3), Brasília, 2006.

BRASIL. Conselho Nacional de Saúde. Resolução 466/12. Trata de pesquisas em seres humanos e atualiza a resolução 196. Diário Oficial da União, 2012. Disponível em: <http://conselho.saude.gov.br/resolucoes/2012/Reso466.pdf>. Acessado em: 13/04/2020.

BRASIL. Manual de gestão de riscos do Tribunal de Contas da União (TCU). – Brasília : TCU, Secretaria de Planejamento, Governança e Gestão (Seplan), 2018.

BRASIL. Instrução Normativa MP/CGU n. 1 de 10/05/2016.

BRASIL. Lei Geral de Telecomunicações, LEI Nº 9.472, 16/07/1997.

BRASIL. Resolução Conjunta nº 1(Aneel, Anatel e ANP), de 24/11/1999.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (COSO). Enterprise Risk Management - Integrated Framework, AICPA: New York, 2004.

CGU. Ministério da Transparência e Controladoria Geral da União. Metodologia de Gestão de Riscos. Brasília, 2018.

COELHO, A. F. C.. As cambiantes relações entre o Estado brasileiro e o setor de telefonia. A&C Revista de Direito Administrativo e Constitucional, Belo Horizonte, ano 6, n. 25, p. 181-212, 2006. DOI: http://dx.doi.org/10.21056/aec.v6i25.433.

COSTA, F. J.; ORSINI, A. C. R.; CARNEIRO, J. S. Variações de Mensuração por Tipos de Escalas de Verificação: Uma Análise do Construto de Satisfação Discente . GESTÃO.Org - Revista Eletrônica de Gestão Organizacional, v. 16, n. 2, p. 132-144, 2018. DOI:http://dx.doi.org/10.21714/1679-18272018v16n2.p132-144

DAVIS, K.; NEWSTROM, J. W. Comportamento humano no trabalho. Vol. 2, São Paulo: Pioneira Thomson Learning, 2001.

DUARTE, C. Uma análise de procedimentos de leitura baseada no paradigma indicichio, 1998. Dissertação (Mestrado em Lingüística) — Instituto de Estudos da Linguagem da Universidade Estadual de Campinas. Campinas.

ESCOBAR, J. C. Mariense Escobar. Serviços de Telecomunicações: Aspectos Jurídicos e Regulatórios. Porto Alegre: Livraria do Advogado Editora, 2005.

ETSI. Nr. 300.392-2 Tetra Air Interface. Paris: ETSI, 2005.

FOX, D. A., Chami, Y., Holmes, N.. Telecommunication networks. U.S. Patent No. 9,654,357, 2017.

FREIRE; JORGE; CANDIDO. Aproximação entre a Ciência da Informação com a Ciência Policial. 1 ed. Cap.VI. Florianópolis, 2019.

GIL, A.C. Como elaborar projetos de pesquisa. 4. ed. São Paulo: Atlas, 2002.

GIL, A.C. Métodos e técnicas de pesquisa social. 5. ed. São Paulo: Atlas, 1999.

KOZIKOSKI, S. M. O Compartilhamento de Infra-Estrutura Relacionado à Prestação do Serviço de Telefonia e a Questão da Remuneração pelo Uso dos Bens Compartilhados. Revista de Direito Administrativo e Constitucional, Belo Horizonte, Ano 4, nº 18, 2004.

KUROWICKA, D., COOKE, R., GOOSSENS, L., & Ale, B. (2008). Expert Judgment study for placement ladder bowtie. Safety Science, volume 46, issue 6, 921-934, 2008.

LAENDER, G. B. Interconexão, Unbundling e Compartilhamento de Meios de Rede de Telecomunicação.Revista de Informação Legislativa. Brasília, Ano 39, nº 154, 2002.

LAUDON, K.; LAUDON, J. Sistemas de Informação Gerenciais. São Paulo: Pearson Prentice Hall, 2010.

LUNA, S. V. O falso conflito entre tendências metodológicas. In: FAZENDA, I. (Org.). Metodologia da pesquisa educacional. 6.ed. São Paulo: Cortez, 2000.

MARCONI, M.A.; LAKATOS, E. M. Metodologia cientifica. 4ªed. São Paulo. Atlas, 2006.

MARKEN, V. B. A Bow-Tie-Based Analysis of the Risk of Delays Along the Northern Sea Route. Marine Technology, 2014.

MASON, J. Introduction: asking difficult questions about qualitative research. In: Qualitative researching, London: Sage Publications, 1997.

MATTAR, F. N. Pesquisa de Marketing, 3 Ed. São Paulo: Atlas, 2001.

MINAYO, M. C. S. Ciência, técnica e arte: o desafio da pesquisa social. In: . (Org.). Pesquisa social: teoria, método e criatividade. 18. ed. Petrópolis: Vozes, 1994.

MONTEIRO, R. C. A pesquisa qualitativa como opção metodológica. Pro-posições, Campinas, n. 5, 1991.

MOTOROLA. L.F. Curso – conceitos trunking, Campinas, 2010.

NASCIMENTO, M. G. O. O compartilhamento da infraestrutura na: Prestação dos Serviços de Telecomunicações, 2013. Disponível em: <https://jus.com.br/artigos/23502/o-compartilhamento-de-infraestrutura-na-prestacao-dos-servicos-de-telecomunicacoes>. Acessado em 15/03/2020.

PMI - PROJECT MANAGEMENT INSTITUTE. Guia PMBOK: Um Guia para o Conjunto de Conhecimentos em Gerenciamento de Projetos, Sexta edição, Pennsylvania: PMI, 2017.

SILVA, A.; RIBEIRO, J.A.; RODRIGUES, L. A. Sistemas de Informação na Administração Pública. Rio de Janeiro: Revan, 2004.

SUNDFELD, C. A. Estudo Jurídico sobre o Preço do Compartilhamento de Infraestrutura de Energia Elétrica. Revista Eletrônica de Direito Administrativo Econômico, Salvador, Instituto de Direito Público da Bahia, vol. 4, 2006.

TANENBAUM, A. S. Redes de Computadores. Editora São Paulo, 2003.

TETRAPOL. Especificação de Avaliação Pública 1.16.1 – Base station to radio switch interface. Paris. Fórum Tetrapol, 2011.

VALLE, R.; OLIVEIRA, S.B. Análise e modelagem de processo de negócio: foco na notação BPMN. Editora Atlas. 2009. Disponível em: <http://pro.poli.usp.br/wp-content/uploads/2012/pubs/analise-e-modelagem-de-processos-de-negocios-para-a-definicao-de-requisitos-de-um-sistema-de-informacao.pdf>. Acessado em: 18/04/2020.

ZANETTI, D. A Cultura do Compartilhamento e a Reprodutibilidade dos Conteúdos. In: Revista Ciberlegenda, v 25, n 2, Editora UFF. 2011.

Apêndice A – Formulário TCLE

PESQUISA

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO (TCLE):

Projeto de Pesquisa: "PROPOSTA DE UM PROCESSO DE AVALIAÇÃO DE RISCOS APLICADO AO COMPARTILHAMENTO DE SISTEMAS DE RADIOCOMUNICAÇÕES DE ÓRGÃOS DE SEGURANÇA PÚBLICA".

Pesquisadores: Dr. André Luiz Castro Leal (Responsável), Aluisio Sardinha Garcia (Mestrando MPGE/UFRRJ). Instituição a que pertence o Pesquisador Responsável: Universidade Federal Rural do Rio de Janeiro. Tel: (21)2681-4938. Telefones para contato com o Pesquisador: (21)2681-4938, e-mail: andrecastr@gmail.com.

O(A) Sr. (a) está sendo convidado (a) a participar do projeto de pesquisa: "PROPOSTA DE UM PROCESSO DE AVALIAÇÃO DE RISCOS APLICADO AO COMPARTILHAMENTO DE SISTEMAS DE RADIOCOMUNICAÇÕES DE ÓRGÃOS DE SEGURANÇA PÚBLICA", sob responsabilidade do pesquisador Prof. Dr. André Luiz Castro Leal. O estudo justifica-se na realização de uma proposta de avaliação de riscos aplicado ao compartilhamento de sistemas de radiocomunicações. Ao identificar e analisar os prováveis riscos, podemos estudar as possíveis falhas ao compartilhar sistemas de radiocomunicações e corrigi-las com antecedência. O compartilhamento de sistemas de radiocomunicações, apesar de não usual, se realizado de forma planejada, poderá trazer benefícios como a facilidade na comunicação entre organizações diferentes e a otimização de custos pela não implantação de novas redes com coberturas redundantes.

O objeto a ser estudado consiste na: "REALIZAÇÃO DE UMA PROPOSTA DE ANÁLISE DE RISCOS APLICADO AO COMPARTILHAMENTO DE SISTEMAS DE RADIOCOMUNICAÇÕES DE UM ÓRGÃO DE SEGURANÇA PÚBLICA", com seguintes objetivos específicos:

1. Realizar um estudo dos modelos de gestão de riscos estabelecidos como a Metodologia de Gestão de Riscos da CGU(2018), as etapas do gerenciamento de riscos segundo o PMBOK(2017) e a Gestão de Riscos segundo a ISO31000(2018);
2. Apresentar uma Proposta de Avaliação de Riscos ao se compartilhar sistemas de radiocomunicações;
3. Elencar os Fatores de Riscos, Eventos de Riscos e Efeitos dos Riscos por meio de uma pesquisa com os gestores da rede de radiocomunicações da Polícia Federal;
4. Analisar o impacto e a probabilidade da ocorrência dos riscos por meio da matriz de riscos;
5. Validar o processo de avaliação de riscos proposto junto aos gestores da área de radiocomunicações da Polícia Federal.

A participação nesta pesquisa é livre, podendo o senhor desistir ou retirar o seu consentimento, sem precisar se justificar, a qualquer momento sem que, contudo, haja prejuízo de qualquer natureza.

A pesquisa não oferecerá riscos para os participantes.

Será garantido o sigilo absoluto dos participantes na pesquisa.

Entendo ter sido eleito a participar desta pesquisa por trabalhar na Polícia Federal e trabalhar na área de radiocomunicação.

Declaro ter conhecimento de que este projeto de conclusão de curso servirá de fonte de informação relevante para o estudo. Informo meu interesse, disponibilidade e concordo em participar desta pesquisa, que garante total anonimato através da utilização de pseudônimos na identificação dos depoimentos.

Afirmo estar ciente de que os resultados da pesquisa serão divulgados em meio científico, e que poderei acessá-los ao final do estudo através do pesquisador e que não receberei qualquer benefício material como resultado de minha participação.

Os participantes de pesquisa, e comunidade em geral, poderão entrar em contato com o Comitê de Ética em Pesquisa da Universidade Federal Rural do Rio de Janeiro para obter informações específicas sobre a aprovação deste projeto ou demais informações: Tel/fax: (21) 2681-4600.

Eu declaro ter sido informado e concordo em participar, como voluntário, do projeto de pesquisa acima descrito.

*Obrigatório

Concorda em participar da pesquisa? *

- ◯ Sim
- ◯ Não

Próxima

Página 1 de 5

Apêndice B – Pergunta 1 do formulário de pesquisa.

PESQUISA

*Obrigatório

1. Na sua opinião, quais são os possíveis riscos (eventos de riscos) existentes ao compartilhar uma rede de radiocomunicações?

ATENÇÃO: Ao final desta página, podem ser inseridos na opção "outros", outros riscos que o entrevistado identifique como risco da Organização ao compartilhar sistemas de radiocomunicações de outras organizações.
Fique a vontade!!! Marque uma ou mais de uma opção abaixo.

- [ ] A rede não suportar o tráfego de novos usuários da Polícia Federal.
- [ ] As informações serem perdidas.
- [ ] As informações perderem o sigilo.
- [ ] A não adaptação aos equipamentos de outra organização.
- [ ] Não saber manusear os equipamentos de outra organização.
- [ ] Os servidores se negarem a usar os equipamentos por serem equipamentos de outra organização.
- [ ] A Polícia Federal não adquirir os equipamentos/acessórios necessários para o uso da nova rede.
- [ ] A cobertura da nova rede não atender a necessidade de cobertura da Polícia Federal.
- [ ] A Polícia Federal não possuir prioridade da rede em situações de congestionamento.
- [ ] A nova rede não disponibilizar o modo tático para operações onde não haja cobertura.
- [ ] A gerência da rede está em outra organização.
- [ ] A falta de autonomia para alterar parâmetros que melhor atendem a Polícia Federal.

- [ ] A não possibilidade de escolha dos fornecedores. Já que os fornecedores já atendem a outra organização.
- [ ] A não possibilidade de fazer uso de criptografia própria.
- [ ] A vulnerabilidade de acesso aos centros de controle de outras organizações.
- [ ] Desconhecimento do pessoal que acessa os centros de controle de outras organizações.
- [ ] O Convênio de compartilhamento ser desfeito sem a devida programação.
- [ ] A não capacitação de servidores na rede a ser compartilhada.
- [ ] A falta de manutenção na rede a ser compartilhada.
- [ ] Desconhecimento da tecnologia usada.
- [ ] Desconhecimento da segurança da rede.
- [ ] Não existem riscos.
- [ ] Outro: _____

Voltar Próxima Página 3 de 5

Apêndice C – Pergunta 2 do formulário de pesquisa.

PESQUISA

*Obrigatório

2. Como você classificaria a probabilidade da ocorrência de determinados riscos (eventos de risco) listados abaixo:

ATENÇÃO: Ao final desta página, podem ser inseridos na opção "outros", outros riscos que o entrevistado identificou na pergunta anterior, indicando logo abaixo, na escala de probabilidade, a sua probabilidade de ocorrência.

Escala de 1 a 5, sendo 1 para a menor probabilidade e 5 para a maior probabilidade.

1 - Raro
2 - Improvável
3 - Possível
4 - Provável
5 - Quase certo

A rede não suportar o tráfego de novos usuários da Polícia Federal. *

1	2	3	4	5
○	○	○	○	○

As informações serem perdidas. *

1	2	3	4	5
○	○	○	○	○

As informações perderem o sigilo. *

1	2	3	4	5
○	○	○	○	○

A não adaptação aos equipamentos de outra organização. *

1	2	3	4	5
○	○	○	○	○

Não saber manusear os equipamentos de outra organização. *

1	2	3	4	5
○	○	○	○	○

Os servidores se negarem a usar os equipamentos por serem equipamentos de outra organização. *

1	2	3	4	5
○	○	○	○	○

A Polícia Federal não adquirir os equipamentos/acessórios necessários para o uso da nova rede. *

1	2	3	4	5
○	○	○	○	○

A cobertura da nova rede não atender a necessidade de cobertura da Organização de Estudo. *

1	2	3	4	5
○	○	○	○	○

A Polícia Federal não possuir prioridade da rede em situações de congestionamento. *

1	2	3	4	5
○	○	○	○	○

A nova rede não disponibilizar o modo tático para operações onde não haja cobertura. *

1	2	3	4	5
○	○	○	○	○

A gerência da rede está em outra organização. *

1	2	3	4	5
○	○	○	○	○

A falta de autonomia para alterar parâmetros que melhor atendem a Polícia Federal. *

1	2	3	4	5
○	○	○	○	○

A não possibilidade de escolha dos fornecedores. Já que os fornecedores já atendem a outra organização. *

1	2	3	4	5
○	○	○	○	○

A não possibilidade de fazer uso de criptografia própria. *

1	2	3	4	5
○	○	○	○	○

A vulnerabilidade de acesso aos centros de controle de outras organizações. *

1	2	3	4	5
○	○	○	○	○

Desconhecimento do pessoal que acessa os centros de controle de outras organizações. *

1	2	3	4	5
○	○	○	○	○

O Convênio de compartilhamento ser desfeito sem a devida programação. *

1	2	3	4	5
○	○	○	○	○

A não capacitação de servidores na rede a ser compartilhada. *

1	2	3	4	5
○	○	○	○	○

A falta de manutenção na rede a ser compartilhada. *

1	2	3	4	5
○	○	○	○	○

Desconhecimento da tecnologia usada. *

1	2	3	4	5
○	○	○	○	○

Desconhecimento da segurança da rede. *

1	2	3	4	5
○	○	○	○	○

Outros (informe abaixo da escala a probabilidade de ocorrência ao risco identificado).

1	2	3	4	5
○	○	○	○	○

Sua resposta

Outros (informe abaixo da escala a probabilidade de ocorrência ao risco identificado).

1	2	3	4	5
○	○	○	○	○

Sua resposta

Voltar Próxima Página 4 de 5

Apêndice D – Pergunta 3 do formulário de pesquisa.

PESQUISA

*Obrigatório

3. Considerando que estes riscos abaixo existem, como você classificaria o impacto destes riscos (eventos de riscos) listados abaixo no compartilhamento de sistemas de radiocomunicações:

ATENÇÃO: Ao final desta página, podem ser inseridos na opção "outros", outros riscos que o entrevistado identificou na primeira pergunta, indicando logo abaixo, na escala de impacto, o seu impacto ao ocorrer o risco identificado.

Escala de 1 a 5, sendo 1 para o menor impacto e 5 para o maior impacto.
1 - Insignificante
2 - Menor
3 - Moderado
4 - Alto
5 - Muito Alto

A rede não suportar o tráfego de novos usuários da Organização de Estudo. *

1	2	3	4	5
○	○	○	○	○

As informações serem perdidas. *

1	2	3	4	5
○	○	○	○	○

As informações perderem o sigilo. *

1	2	3	4	5
○	○	○	○	○

A não adaptação aos equipamentos de outra organização. *

1	2	3	4	5
○	○	○	○	○

Não saber manusear os equipamentos de outra organização. *

1	2	3	4	5
○	○	○	○	○

Os servidores se negarem a usar os equipamentos por serem equipamentos de outra organização. *

1	2	3	4	5
○	○	○	○	○

A Polícia Federal não adquirir os equipamentos/acessórios necessários para o uso da nova rede. *

1	2	3	4	5
○	○	○	○	○

A cobertura da nova rede não atender a necessidade de cobertura da Organização de Estudo. *

1	2	3	4	5
○	○	○	○	○

A Polícia Federal não possuir prioridade da rede em situações de congestionamento. *

1	2	3	4	5
○	○	○	○	○

A nova rede não disponibilizar o modo tático para operações onde não haja cobertura. *

1	2	3	4	5
○	○	○	○	○

A gerência da rede está em outra organização. *

1	2	3	4	5
○	○	○	○	○

A falta de autonomia para alterar parâmetros que melhor atendem a Polícia Federal. *

1	2	3	4	5
○	○	○	○	○

A não possibilidade de escolha dos fornecedores. Já que os fornecedores já atendem a outra organização. *

1	2	3	4	5
○	○	○	○	○

A não possibilidade de fazer uso de criptografia própria. *

1	2	3	4	5
○	○	○	○	○

A vulnerabilidade de acesso aos centros de controle de outras organizações. *

1	2	3	4	5
○	○	○	○	○

Desconhecimento do pessoal que acessa os centros de controle de outras organizações. *

1	2	3	4	5
○	○	○	○	○

O Convênio de compartilhamento ser desfeito sem a devida programação. *

1	2	3	4	5
○	○	○	○	○

A não capacitação de servidores na rede a ser compartilhada. *

1	2	3	4	5
○	○	○	○	○

A falta de manutenção na rede a ser compartilhada. *

1	2	3	4	5
○	○	○	○	○

Desconhecimento da tecnologia usada. *

1	2	3	4	5
○	○	○	○	○

Desconhecimento da segurança da rede. *

1	2	3	4	5
○	○	○	○	○

Outros (informe abaixo da escala a probabilidade de ocorrência ao risco identificado).

1	2	3	4	5
○	○	○	○	○

Sua resposta

Outros (informe abaixo da escala a probabilidade de ocorrência ao risco identificado).

1	2	3	4	5
○	○	○	○	○

Sua resposta

Sua resposta será enviada, confirma? *

- ○ sim, quero enviar minhas respostas agora.
- ○ Não, quero Refazer/Revisar minhas respostas.

Voltar Próxima Página 5 de 5

PESQUISA

MUITO OBRIGADO!!!!
Suas respostas foram registradas!!!

Apêndice E – Termo de Anuência para Autorização da Pesquisa.

UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
INSTITUTO DE CIÊNCIAS SOCIAIS APLICADAS
MESTRADO PROFISSIONAL EM GESTÃO E ESTRATÉGIA
TERMO DE ANUÊNCIA PARA AUTORIZAÇÃO DE PESQUISA

Prezado Sr. WILLIAM MARCEL MURAD,

Solicitamos autorização para realização da pesquisa intitulada "PROPOSTA DE UM PROCESSO UNIFICADO DE GESTÃO DE RISCOS APLICADO AO COMPARTILHAMENTO DE REDES DE RADIOCOMUNICAÇÕES DE ÓRGÃOS DE SEGURANÇA" a ser realizada pelo discente Aluisio Sardinha Garcia do Mestrado Profissional em Gestão e Estratégia (MPGE/UFRRJ), sob a orientação do Prof. Dr. Andre Luiz de Castro Leal, visando ter acesso aos dados a serem colhidos em sua Diretoria.

Informamos que as informações a serem colhidas na forma de documentos, informativos e entrevistas servirão de subsídios para a elaboração de artigos de natureza acadêmico científica, podendo ser apresentados como trabalho em eventos (congressos, seminários, conferencias, et.) ou publicados em revistas da mesma natureza, mantendo as ressalvas quanto as informações resguardadas quanto à natureza de atuação do órgão.

Declaramos conhecer e cumprir as Resoluções Éticas brasileiras e salientamos que os dados coletados serão utilizados para o fim descrito neste documento.

Na certeza de contarmos com a sua colaboração e empenho agradecemos antecipadamente a atenção e nos disponibilizamos para quaisquer esclarecimentos que se fizerem necessários.

Rio de Janeiro, 12 de abril de 2019.

Andre Luiz de Castro Leal
Docente Responsável pela pesquisa – MPGE/UFRRJ

Aluisio Sardinha Garcia
Mestrando – MPGE/UFRRJ

( ) Concordo com a pesquisa e com a utilização do nome da Polícia Federal.

( ) Concordo com a pesquisa, mas solicito a não inclusão da Polícia Federal.

William Marcel Murad
Diretor de Tecnologia da Informação e Inovação da Polícia Federal

Apêndice F – Autorização de uso do Nome da Polícia Federal na Pesquisa.

aluisio.asg@dpf.gov.br

De: Imprensa Dcs <imprensa@dpf.gov.br>
Enviado em: sexta-feira, 21 de junho de 2019 15:17
Para: Aluisio Sardinha Garcia
Assunto: Re: Informações para Uso do Nome da Polícia Federal em Pesquisa de Mestrado

Prezado Sr. Aluisio Sardinha Garcia,

Diante do cenário apresentado, a Divisão de Comunicação Social não vê óbice que o nome da instituição seja citado na obra em produção.

Em muitos casos, quando nossos servidores produzem obras acadêmicas e literárias, sobre suas experiências profissionais, fica impossível que não haja citações à instituição.

Claro que a anuência do órgão passa também pelo respeito à política de comunicação social da PF, consagrada pela IN 013/2018, disponível em http://intranet.dpf.gov.br/institucional/marcas/IN_13_08.pdf/view
sugere-se sua leitura atenta.

As recomendações que seguimos e repassamos são as de praxe, ligadas ao bom senso e à IN citada:

Não citar nomes de policiais e investigados (pessoas físicas ou jurídicas)
Não detalhar métodos de investigação.
Evitar comentários sobre outros órgãos e poderes da República.
Evitar opiniões pessoais (procurar comentar apenas situações em tese).

Seguimos à disposição para qualquer dúvida que persista.

Cordialmente,
--

***Fabio** Ricardo Hegenbart Bueno* (matrícula: 8.275)
Agente de Polícia Federal | Departamento de Polícia Federal
--
Assessoria de Comunicação
Divisão de Comunicação Social
(61) 2024-8142

POLÍCIA FEDERAL
www.pf.gov.br

Em Sexta, Junho 21, 2019 13:41 -03, "Aluisio Sardinha Garcia" <aluisio.asg@dpf.gov.br> escreveu:

Prezados,
boa tarde.

tem um posicionamento sobre o solicitado?
Atenciosamente,
Aluisio Sardinha Garcia
21 991195853

Em Terça, Junho 18, 2019 15:32 -03, "Aluisio Sardinha Garcia" <aluisio.asg@dpf.gov.br> escreveu:

Senhor Chefe da Comunicação Social,
APF Fabio Bueno,
boa tarde.

Meu nome é Aluisio Sardinha Garcia, sou ATE, matricula DPF 13.356 e lotado no STI/SR/PF/RJ.
Atualmente curso o Mestrado de Gestão e Estratégia/PPGGE na UFRRJ na linha de pesquisa Gestão de Processos, Projetos e Tecnologias.

Para ingressar nos estudos fui autorizado pelo Senhor Superintendente Regional do Rio de Janeiro (SR/PF/RJ) por meio do processo SEI 08455.033102/2017-21.

O titulo da pesquisa é: PROPOSTA DA REALIZAÇÃO DA GESTÃO DE RISCOS APLICADO AO COMPARTILHAMENTO DE REDES DE RADIOCOMUNICAÇÕES DE ÓRGÃOS DE SEGURANÇA.

Para realizar as entrevistas com os Gestores de Radiocomunicação dos estados, recebi no processo SEI 08455.014054/2019-34 a autorização por meio do **Termo de Anuência para Autorização de Pesquisa** assinado pelo senhor Diretor Tecnologia e Inovação (DTI/DG).

Ocorre que por se tratar de um mestrado profissional, onde a pesquisa a ser realizada procura buscar o intercâmbio entre as atividades funcionais vinculadas ao servidor com o meio acadêmico, fica quase impossível não associar o nome da Polícia Federal no texto escrito na dissertação de mestrado.

Considerando as informações aqui descritas, gostaria de buscar informações sobre o uso do nome da Polícia Federal no texto da dissertação de Mestrado em andamento.

Desde já grato,

Cordialmente,
Aluisio Sardinha Garcia
Agente de Telecomunicações
Matr. 13.356
21 991198583

Apêndice G – Aprovação do Comitê de Ética em pesquisa da UFRRJ.

SERVIÇO PÚBLICO FEDERAL
UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
COMITÊ DE ÉTICA EM PESQUISA DA UFRRJ / CEP

Protocolo N° 1.431/19

PARECER

O Projeto de Pesquisa intitulado "Proposta de um processo unificado de gestão de riscos aplicado ao compartilhamento de sistemas de radiocomunicações de órgãos de segurança" sob a coordenação do Professor Dr. Andre Luiz de Castro Leal, do Instituto de Ciências Sociais Aplicadas/Programa de Pós-Graduação em Gestão e Estratégia, processo 23083.034817/2019-22, atende os princípios éticos e está de acordo com a Resolução 466/12 que regulamenta os procedimentos de pesquisa envolvendo seres humanos.

UFRRJ, 22/01/2020.

Prof.ª Dra. Lúcia Helena Cunha dos Anjos
Pró-Reitora Adjunta de Pesquisa e Pós-Graduação

Apêndice H – Relatório Técnico Final da Pesquisa.

Resumo

Este relatório técnico científico possui o objetivo de trazer os resultados de uma forma mais direta da dissertação intitulada: “Proposição, aplicação e validação de um framework de avaliação de riscos, aplicado ao compartilhamento de sistemas de radiocomunicações de um órgão de segurança pública.” Por meio de um modelo mais ágil de acesso aos dados mais relevantes da pesquisa, este relatório contribui para o uso efetivo dos resultados encontrados ao fim da pesquisa, esses resultados são facilmente encontrados em um relatório técnico final da pesquisa.

1- Introdução

O fomento à pratica do compartilhamento de sistemas de radiocomunicações contribui para o uso racional dos recursos públicos, evita as diversas redes sobrepostas tornando mais eficiente o uso de sistemas já instalados de outras forças de segurança.

No entanto muitas organizações incentivam a instalação de novas redes devido as incertezas encontradas ao se compartilhar sistemas já instalados, mesmo que isso represente uma economia nos projetos de novas redes.

A análise de riscos ao mitigar as incertezas desse compartilhamento, segundo Freire, Jorge e Candido (2019), contribui para aumentar a viabilidade do compartilhamento de sistemas de radiocomunicações entre organizações.

O desenvolvimento do relatório apresentará os seguintes resultados: entrega do macroprocesso e seus subprocessos; identificação dos eventos de risco; indicação das escolhas dos eventos de risco pelos respondentes; identificação dos fatores de risco, efeitos de risco e seus Controles; apresentação dos controles pós validação e apresentação da matriz de risco final após aplicação dos controles e validado pelos especialistas.

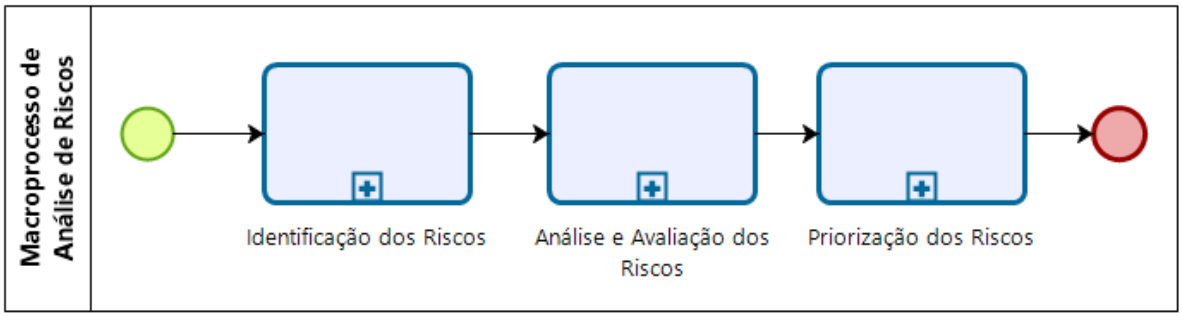
2- Desenvolvimento

Entrega do macroprocesso e seus subprocessos

O primeiro resultado da pesquisa foi o desenvolvimento do macroprocesso de Análise de Riscos que foi validado posteriormente, para o desenvolvimento desse macroprocesso tomou se como base três normativas, com maior aderência à normativa da CGU mas com influências do PMBOK e ISO31000.

A estrutura do macroprocesso definido é apesentada na figura abaixo.

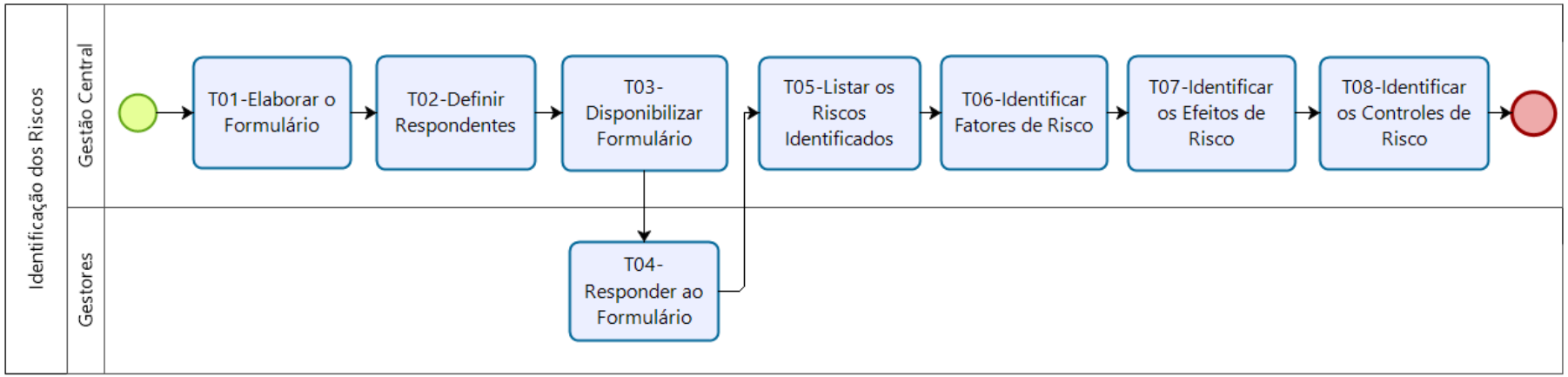
Macroprocesso de Análise de Riscos e seus subprocessos.



Fonte: Elaborada pelo autor (*BPMNotation*), 2019.

O próximo passo foi a definição dos subprocessos que compõe o macroprocesso de Análise de Riscos, são eles os subprocessos de Identificação dos Riscos, de Análise e Avaliação dos Riscos e o de Priorização dos Riscos.

Subprocesso de Identificação dos Riscos.



Fonte: Elaborada pelo autor (*BPMNotation*), 2020.

T01-Elaborar Formulário: é a atividade onde é elaborado o formulário para serem passados aos gestores para a identificação dos efeitos de risco.

T02-Definir os Respondentes: é a atividade onde, com base em critérios pré-estabelecidos, se define os respondentes da pesquisa.

T03-Disponibilizar Formulário: é a atividade onde a identificação dos fatores de risco foi realizada por meio do levantamento de campo, onde um formulário *on-line* foi disponibilizado para os respondentes.

T04-Responder ao Formulário: é a atividade onde os respondentes respondem ao formulário para identificar os riscos, suas probabilidades de ocorrência e seus impactos ao ocorrerem.

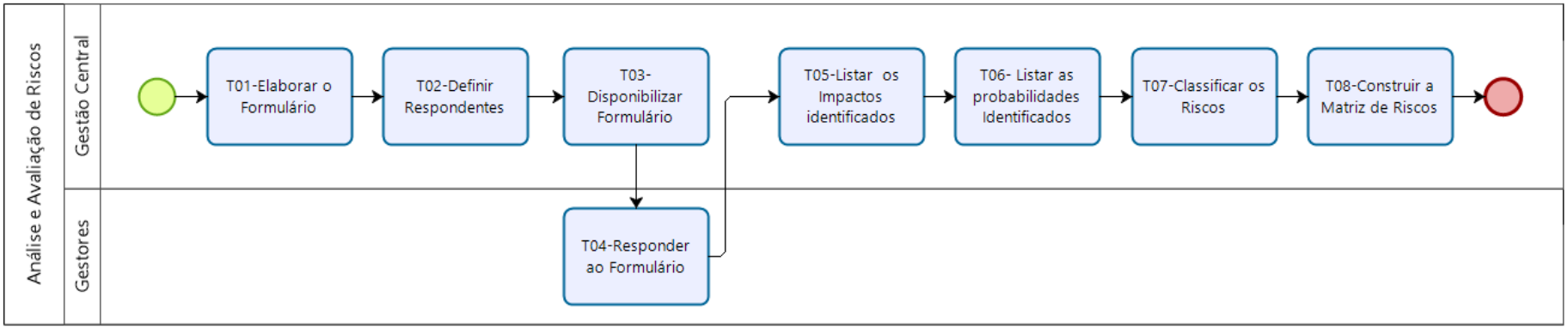
T05-Listar os Riscos Identificados: é a atividade que recebe os riscos levantados pelos respondentes e cria uma lista com esses riscos.

T06-Identificar os Fatores de Risco: é a atividade onde a gestão central identifica os fatores de risco, as causas que levaram a ocorrência destes riscos, nesta pesquisa foi realizada pelo pesquisador.

T07-Identificar os Efeitos de Risco: é a atividade onde a gestão central identifica os Efeitos de Risco, as consequências da ocorrência destes riscos, nesta pesquisa foi realizada pelo pesquisador.

T08-Identificar os Controles de Risco: é a atividade onde a gestão central identifica os Controles de Risco, podendo ser controles preventivos de risco e controles reativos dos riscos, nesta pesquisa foi realizada pelo pesquisador.

Subprocesso de Análise e Avaliação dos Riscos.



Fonte: Elaborada pelo autor (*BPMNotation*), 2020.

T01-Elaborar o Formulário: é a atividade onde é elaborado o formulário para serem passados aos gestores para a identificação dos efeitos de risco. Esta atividade está apenas ilustrada nesse subprocesso para sua identificação e existência, esta atividade é realizada na subprocesso de identificação de riscos.

T02-Definir os Respondentes: é a atividade onde, com base em critérios pré-estabelecidos, se define os respondentes da pesquisa. Esta atividade está apenas ilustrada nesse subprocesso para sua identificação e existência, esta atividade é realizada na subprocesso de identificação de riscos.

T03-Disponibilizar Formulário: é a atividade onde a identificação dos fatores de risco foi realizada por meio do levantamento de campo, onde um formulário *on-line* foi disponibilizado para os respondentes. Esta atividade está apenas ilustrada nesse subprocesso para sua identificação e existência, esta atividade é realizada na subprocesso de identificação de riscos.

T04-Responder ao Formulário: é a atividade onde os respondentes respondem ao formulário para identificar os riscos, suas probabilidades de ocorrência e seus impactos ao ocorrerem.

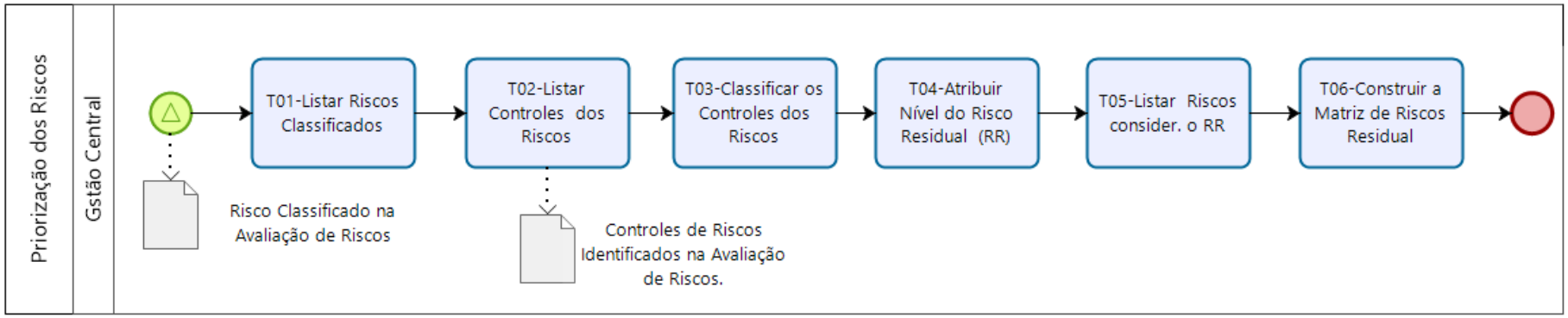
T05-Listar os Impactos Identificados: é a atividade onde se recebe os impactos aos riscos levantados pelos respondentes e identifica em uma lista os impactos para cada risco identificado.

T06-Listar as Probabilidades Identificadas: é a atividade onde se recebe as probabilidades aos riscos levantados pelos respondentes e identifica em uma lista as probabilidades para cada risco identificado.

T07-Classificar os Riscos: é a atividade onde a gestão central classifica os riscos em Risco Extremo, Risco Alto, Risco Médio e Risco Baixo em função do produto da probabilidade de ocorrência e o impacto dos riscos identificados.

T08-Construir a Matriz de Risco: é a atividade onde a gestão central constrói a Matriz de Riscos em função dos níveis riscos classificados na atividade anterior, nesta pesquisa foi realizada pelo pesquisador.

Subprocesso Priorização dos Riscos.



Fonte: Elaborada pelo autor (*BPMNotation*), 2020.

T01-Listar Riscos Classificados: é a atividade onde são recebidos os Risco Classificado no subprocesso de Avaliação de Riscos.

T02-Listar Controles dos Riscos: é a atividade onde são listados os controles de riscos identificados no subprocesso de Avaliação de Riscos.

T03-Classificar os Controles de Risco: é a atividade onde são avaliados os controles de risco identificados no subprocesso de Identificação de Riscos conforme preconiza o normativo da Metodologia de Gestão de Riscos CGU (2018).

T04-Atribuir Nível do Risco Residual: é a atividade onde o nível de risco recebe o fator dado ao controle de risco e o efeito de risco recebe um novo nível de risco, o Risco Residual.

T05-Listar Riscos Considerando RR: é a atividade onde é listado o nível do evento de risco considerando o Risco Residual.

T06-Listar as Probabilidades Identificadas: é a atividade que recebe as probabilidades aos riscos levantados pelos respondentes e identifica em uma lista as probabilidades para cada risco identificado.

T07-Classificar os Riscos: é a atividade onde a gestão central classifica os riscos em Risco Extremo, Risco Alto, Risco Médio e Risco Baixo em função do produto da probabilidade de ocorrência e o impacto dos riscos identificados.

T08-Construir a Matriz de Risco Residual: é a atividade onde a gestão central constrói a Matriz de Riscos Residual em função dos níveis riscos classificados na atividade anterior, nesta pesquisa foi realizada pelo pesquisador.

Identificação dos Eventos de Risco

O próximo resultado foi a identificação dos eventos de risco, foram identificados ao final da pesquisa 21 eventos de risco que estão listados no Quadro abaixo, nesse quadro é possível identificar os eventos de risco em função de sua fase de identificação: os identificados pelo pesquisador previamente; os identificados na etapa de calibragem e os identificados durante a pesquisa.

Eventos de risco.

	Eventos de Risco
1	A rede não suportar o tráfego de novos usuários da Polícia Federal.
2	As informações serem perdidas.
3	As informações perderem o sigilo.
4	A não adaptação aos equipamentos de outra organização.
5	Não saber manusear os equipamentos de outra organização.
6	Os servidores se negarem a usar os equipamentos por serem equipamentos de outra organização.
7	A Polícia Federal não adquirir os equipamentos/acessórios necessários para o uso da nova rede.
8	A cobertura da nova rede não atender a necessidade de cobertura da Polícia Federal.
9	A Polícia Federal não possuir prioridade da rede em situações de congestionamento.
10	A nova rede não disponibilizar o modo tático para operações onde não haja cobertura.
11	O Convênio de compartilhamento ser desfeito sem a devida programação.
12	A gerência da rede está em outra organização.
13	A falta de autonomia para alterar parâmetros que melhor atendem a Polícia Federal.
14	A não possibilidade de escolha dos fornecedores. Já que os fornecedores já atendem a outra organização.
15	A não possibilidade de fazer uso de criptografia própria.
16	A vulnerabilidade de acesso aos centros de controle de outras organizações.
17	Desconhecimento do pessoal que acessa os centros de controle de outras organizações.
18	A não capacitação de servidores na rede ser compartilhada
19	A falta de manutenção da rede compartilhada
20	Desconhecimento da tecnologia usada
21	Desconhecimento da Segurança da Rede
	Não existirem riscos

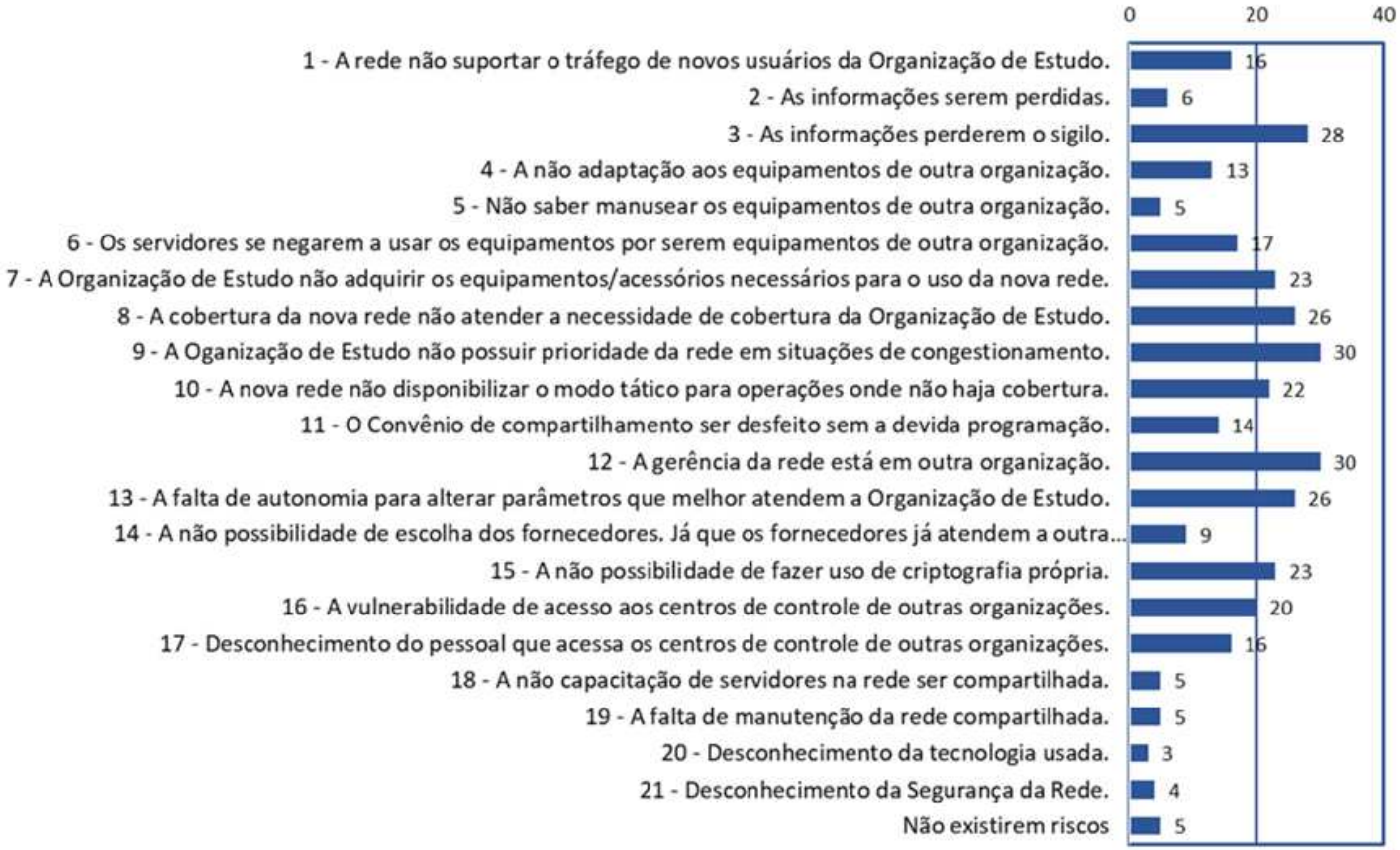
Identificados pelo pesquisador | Identificados na etapa de calibragem | Identificados durante a pesquisa

Fonte: Extraído dos resultados da pesquisa de campo, 2019.

Indicação dos Eventos de Risco pelos respondentes

A Figura abaixo apresenta a indicação dos respondentes pelos eventos de risco disponibilizados na pesquisa, além dos eventos de riscos identificados existiram respondentes que fizeram a opção de “Não existirem riscos”, por acreditar que não existem riscos ao compartilhar redes de radiocomunicações.

Indicação dos Eventos de Risco pelos respondentes na pesquisa de campo.



Fonte: Extraída dos resultados da pesquisa de campo, 2019.

Identificação dos Fatores de Risco, Efeitos de Risco e seus Controles.

O outro resultado alcançado foi a identificação das causas, chamadas de fatores de riscos, os efeitos de risco causados pelos eventos de riscos identificados e seus controles, os preventivos e reativos.

No Quadro abaixo, os resultados são pós validação dos especialistas, na busca de maior relevância de tratamento dos resultados encontrados, somente se buscou resultados dos eventos de risco que receberam mais de 5 indicações.

Identificação dos fatores e efeito de risco e seus controles com contribuição dos especialistas que participaram da validação.

Evento de Risco 1 - A rede não suportar o tráfego de novos usuários da Polícia Federal.			
Fatores	Poucos canais disponíveis. Muitos usuários usando a rede numa mesma região. A rede não foi planejada para ser compartilhada. Falta de manutenção da rede.	Preventivo	Instalar maior número de canais. Planejar a comunicação de operações integradas. Prever maior número de canais quando da entrada de novos parceiros na rede. Criar o ciclo de manutenção preventiva do sistema.
Efeito	Equipes incomunicáveis. Congestionamento da rede.	Reativo	Elaborar comunicação de contingência. Coordenar o fluxo prioritário de comunicação da rede.
Evento de Risco 2 - As informações serem perdidas.			
Fatores	Inoperância a rede. Perda de backup das informações. O não acesso ao core da rede.	Preventivo	Elaborar comunicação de contingência. Criação de rotinas de backups. Negociar o compartilhamento do core da rede.
Efeito	Falta de informações de uso da rede pelos usuários. Atraso nas respostas das demandas dos usuários.	Reativo	Busca acesso aos backups. Busca de dados em local fora de sistemas. Colocar o sistema anterior para funcionar.
Evento de Risco 3 - As informações perderem o sigilo.			
Fatores	Acesso não autorizado nas bases do sistema. Uso de equipamentos de rádio não autorizado. Escuta não autorizado de informações da organização. Quebra da criptografia.	Preventivo	Identificação dos acessos e trocas de senhas periódicas. Possuir controle de uso de rádios dos usuários. Buscar protocolos de restrição de acesso aos dados da organização. Atualização das criptografias do sistema.
Efeito	Acesso não autorizado das informações da organização.	Reativo	Uso de códigos nas comunicações que dificultem o entendimento das informações trafegadas.

Evento de Risco 4 - A não adaptação aos equipamentos de outra organização.			
Fatores	Equipamentos diferentes dos usualmente usados. Falta de treinamento nos novos equipamentos. Falta de acessórios úteis a missão da organização. Equipamentos não adaptados a missão da organização.	Preventivo	Realizar treinamento nos novos equipamentos. Realizar treinamento nos novos equipamentos. Buscar os acessórios necessários ao cumprimento à missão da organização. Buscar equipamentos na nova rede que atendam as particularidades da organização.
Efeito	Os servidores não usarem os novos equipamentos. Busca de um sistema que atenda das necessidades da organização.	Reativo	Campanhas de uso e importância do da comunicação numa organização de segurança. Continuar prospectando sistema de comunicação próprio.
Evento de Risco 6 - Os servidores se negarem a usar os equipamentos por serem equipamentos de outra organização.			
Fatores	Não adaptação aos equipamentos. Falta de treinamento. Rejeição ao uso de novos equipamentos.	Preventivo	Campanhas de uso e importância do da comunicação numa organização de segurança. Realizar treinamentos de uso dos equipamentos. Campanhas de uso e importância do da comunicação numa organização de segurança.
Efeito	Os servidores não usarem os novos equipamentos. As operações ficarem sem comunicação.	Reativo	Realizar treinamento nos novos equipamentos. Baixar normativos que obriguem os servidores a usar.
Evento de Risco 7 - A Polícia Federal não adquirir os equipamentos/acessórios necessários para o uso da nova rede.			
Fatores	Falta de recursos para compra dos equipamentos/acessórios. Não serem disponibilizados pelo fornecedor equipamentos / acessórios de acordo com a particularidade da organização.	Preventivo	Buscar orçamento justificando a necessidade do recurso para compra dos equipamentos / acessórios que atendam a necessidade da organização. Buscar com outros fornecedores equipamentos / acessórios que atendam a necessidade da organização.
Efeito	Os servidores não usarem os novos equipamentos.	Reativo	Campanhas de uso e importância do da comunicação numa organização de segurança até que se busque os equipamentos/acessórios que atendam a necessidade da organização.
Evento de Risco 8 - A cobertura da nova rede não atender a necessidade de cobertura da Polícia Federal.			
Fatores	Falhas de estações. Não previsão dos locais que interessam a organização nos projetos de instalação.	Preventivo	Buscar orçamento justificando a necessidade do recurso para compra dos equipamentos/acessórios que atendam a necessidade da organização. Buscar com outros fornecedores de equipamentos/acessórios que atendam a necessidade da organização.

Efeito	Falta de cobertura nos locais de atuação da organização. Os servidores não usarem os novos equipamentos.	Reativo	Buscar junto ao gestor da rede a instalação de novas estações de transmissão que atendam a organização. Campanhas de uso e importância do da comunicação numa organização de segurança até que se obtenha coberturas que atendam a necessidade da organização.
Evento de Risco 9 - A Polícia Federal não possuir prioridade da rede em situações de congestionamento.			
Fatores	A não previsão de prioridade da rede no projeto de instalação do sistema. Falta de disponibilidade de canais de comunicação.	Preventivo	Solicitar junto ao gestor da rede a prioridade dos canais. Aumento do número de canais da rede.
Efeito	Os servidores não conseguirem usar a rede de comunicação.	Reativo	Busca de um sistema de comunicação de contingencias.
Evento de Risco 10 - A nova rede não disponibilizar o modo tático para operações onde não haja cobertura			
Fatores	O sistema não disponibilizar sistema tático. A Polícia Federal não adquirir o sistema tático.	Preventivo	Buscar um sistema de contingencias que supra o modo tático Realizar estudos para a compra do sistema tático. Manter o sistema tático atual.
Efeito	Falta de cobertura em áreas remotas.	Reativo	Busca de um sistema de contingencias para suprir o modo tático.
Evento de Risco 11 - O Convênio de compartilhamento ser desfeito sem a devida programação.			
Fatores	Falta de gerencia dos prazos do contrato. Descumprimento dos acordos do contrato. Não atendimento das necessidades de comunicação da organização.	Preventivo	Manter os cuidados com os prazos e gerencia dos prazos junto a organização parte do contrato. Manter os cuidados para o cumprimento dos acordos contratuais da organização previstos no contrato. Buscar sistemas de contingencias e prospectar sistemas próprios de comunicação.
Efeito	Os servidores não conseguirem usar a rede de comunicação.	Reativo	Busca de um sistema de comunicação de contingencias.
Evento de Risco 12 - A gerência da rede está em outra organização.			
Fatores	A organização ser a detentora da gerência da rede. O sistema não permitir espelhamento da gerencia da rede. O sistema ter sido comprado por	Preventivo	Buscar junto à organização que gerencia a rede acesso aos controles da rede. Buscar junto à organização o espelhamento da gerencia do sistema.

	outro órgão.		
Efeito	Não ser possível customizar a rede como as alterações que melhor atendem a organização.	Reativo	Buscar junto à organização que possui a gerencia da rede as possibilidades de customizar a rede para que melhor possa atender a Polícia Federal.
Evento de Risco 13 - A falta de autonomia para alterar parâmetros que melhor atendem a Polícia Federal.			
Fatores	A organização ser a detentora da gerência da rede. Não ser previsto em contrato a autonomia necessária para alterações de parâmetros que melhor atendem a Polícia Federal.	Preventivo	Buscar junto à organização que gerencia a rede acesso aos controles da rede. Buscar instruir cláusulas no contrato de compartilhamento que permitam a Polícia Federal alterar parâmetros que melhor lhe atendam.
Efeito	Não ser possível customizar a rede como as alterações que melhor atendem a organização. Os servidores não conseguirem usar a rede de comunicação.	Reativo	Buscar junto à organização que possui a gerencia da rede as possibilidades de customizar a rede para que melhor possa atender a Polícia Federal. Busca de um sistema de comunicação de contingencias.
Evento de Risco 14 - A não possibilidade de escolha dos fornecedores. Já que os fornecedores já atendem a outra organização.			
Fatores	O contrato pertencer a outra organização. A Polícia Federal não possuir interesse em ter uma rede própria.	Preventivo	Busca aproximação aos fornecedores para atender as necessidades da PF. Prospectar uma rede de radiocomunicação própria.
Efeito	Fornecedores com propostas engessadas de preço e disponibilidade de material diferenciado.	Reativo	Prover gestões junto aos fornecedores materiais que atenda a organização com preços de mercado.
Evento de Risco 15 - A não possibilidade de fazer uso de criptografia própria.			
Fatores	A criptografia já vier inserida no sistema contratado. O gerador de chaves criptográficas não ficar instalado na Polícia Federal. O sistema não possibilitar instalar criptografia própria.	Preventivo	Buscar junto à organização que gerencia o sistema a possibilidade de instalar uma criptografia própria da Polícia Federal. Buscar junto à organização que gerencia o sistema instalar na Polícia Federal o gerador de chaves criptográficas. Buscar junto aos fornecedores e ao gestor do sistema de comunicações os meios para instalar uma criptografia própria.
Efeito	A Polícia Federal fazer uso de uma criptografia comum na organização. Os servidores não usarem os novos equipamentos. As comunicações perderem o sigilo.	Reativo	Fazer uso de controle controles de segurança próprios dos equipamentos que possibilitem a customização para a atividade da Polícia Federal. Buscar de novos equipamentos que atendam a organização.

Evento de Risco 16 - A vulnerabilidade de acesso aos centros de controle de outras organizações.			
Fatores	Os centros de controle estar em outra organização. Desconhecimento dos controles aplicados pela organização que gerencia o sistema.	Preventivo	Buscar informações e combinar protocolos de acesso com a outra organização. Buscar informações e participar dos controles que existem nos centros de controle.
Efeito	As informações trafegadas pela organização estarem expostas.	Reativo	Procurar fazer uso de códigos na comunicação.
Evento de Risco 17 - Desconhecimento do pessoal que acessa os centros de controle de outras organizações.			
Fatores	Não participar da seleção de pessoas que acessam o sistema. A gestão do centro de controle não estar na Polícia Federal.	Preventivo	Buscar informações das pessoas que acessam os centros de controle. Buscar informações das pessoas que acessam os centros de controle.
Efeito	As informações trafegadas pela organização estarem expostas. As comunicações erderem o sigilo.	Reativo	Procurar fazer uso de códigos na comunicação.

Fonte: Elaborado pelo autor, 2020.

Definição dos controles pós validação

A etapa seguinte procurou validar os níveis dos controles internos levantados na pesquisa para a definição dos fatores de avaliação dos riscos identificados na pesquisa.

Para esta etapa da validação os respondentes foram especialistas que avaliaram cada controle dos Fatores de Riscos identificados anteriormente.

Foram definidos os seguintes controles após validação dos resultados obtidos preliminarmente na pesquisa, esses resultados são apresentados na coluna “Resultado”, com o seu respectivo fator ao lado definido.

Em seguida abaixo é apresentado a matriz de risco final após validação e com todas as correções que sofreram no processo.

Para a construção da matriz de riscos, os valores usados para probabilidade e impacto foram retirados a partir da moda dos resultados, o produto da probabilidade X impacto e a sua classificação de eventos de risco e suas cores são: verde para risco baixo (RB); amarelo para risco médio (RM); laranja para risco alto (RA) e vermelho para risco extremo (RE).

Valores do produto da probabilidade X impacto COM controle e sua classificação atribuídos na validação pelos especialistas.

				Valores Produto Prob x Imp			
	Eventos de Risco	Resultado	Fator	Valores SEM controle	Valores COM controle ANTES Validação	Valores COM controle APÓS Validação	Classificação PÓS Validação
ER-1	A rede não suportar o tráfego de novos usuários da Polícia Federal.	Inexistente	1	40	40	40	RA
ER-2	As informações serem perdidas.	Inexistente	1	20	16	20	RM
ER-3	As informações perderem o sigilo.	Inexistente	1	50	50	50	RA
ER-4	A não adaptação aos equipamentos de outra organização.	Inexistente	1	25	25	25	RM
ER-6	Os servidores se negarem a usar os equipamentos de outra organização.	Inexistente	1	10	10	10	RM
ER-7	A Polícia Federal não adquirir os equipamentos/acessórios necessários.	Inexistente	1	40	40	40	RA
ER-8	A cobertura da nova rede não atender a necessidade de cobertura da Polícia Federal.	Inexistente	1	80	80	80	RE
ER-9	A Polícia Federal não possuir prioridade da rede em situações de congestionamento.	Inexistente	1	50	40	50	RA
ER-10	A nova rede não disponibilizar o modo tático para operações onde não haja cobertura.	Fraco	0,8	64	38,4	51,2	RA
ER-11	O Convênio de compartilhamento ser desfeito sem a devida programação.	mediano	0,6	40	24	24	RM
ER-12	A gerência da rede está em outra organização.	Fraco	0,8	25	25	20	RM
ER-13	A falta de autonomia para alterar parâmetros que melhor atendem a Polícia Federal.	Inexistente	1	64	51,2	64	RA
ER-14	A não possibilidade de escolha dos fornecedores.	Fraco	0,8	50	40	40	RA
ER-15	A não possibilidade de fazer uso de criptografia própria.	Fraco	0,8	40	32	32	RM
ER-16	A vulnerabilidade de acesso aos centros de controle de outras organizações.	Inexistente	1	50	40	50	RA
ER-17	Desconhecimento do pessoal que acessa os centros de controle de outras organizações.	Inexistente	1	40	32	40	RA

Risco Baixo | Risco Médio | Risco Alto | Risco Extremo

Fonte: Extraído dos resultados da pesquisa, 2020.

Matriz de Risco – COM controle – APÓS Especialistas

Impacto						
	Muito Alto 10		ER2-20	ER3-50 ER14-40 ER16-50	ER8-80	
	Alto 8			ER1-40 ER7-40 ER9-50	ER13-64	
	Moderado 5			ER4-25 ER11-24 ER12-20	ER10-51,2	ER17-40
	Pequeno 2			ER6-10	ER-15-32	
	Insignificante 1					
		Raro 1	Improvável 2	Possível 5	Provável 8	Muito Alto 10
		Probabilidade				

Risco Baixo | Risco Médio | Risco Alto | Risco Extremo

Fonte: Extraída dos resultados da pesquisa, 2020.

3- Resultados e conclusões

Foi possível demostrar os principais resultados da pesquisa por meio deste relatório, o que facilita uma busca rápida e direta dos principais objetivos da pesquisa alcançados.

Estes resultados contribuem para facilitar o compartilhamento de sistemas de radiocomunicações entre forças de segurança e auxiliar na elaboração de processos específicos de análise de riscos destes compartilhamentos.

Essa análise de riscos contribui para que as organizações passem a pisar em solo conhecido, contribuindo com a viabilidade do compartilhamento de sistemas de radiocomunicações entre organizações de segurança pública e defesa no Brasil.

Este relatório contribui para difundir os resultados dessa pesquisa tanto no meio acadêmico, como na organização de estudo e em organizações similares a organização estudada.