Revista Brasileira de Administração Científica
Brazilian Journal of Scientific Administration

Out a Dez 2020 - v.11 - n.4

ISSN: **2179-684X**

This article is also available online at:
www.sustenere.co

Identificação dos eventos, fatores e efeitos de risco ao compartilhar sistemas de radiocomunicações entre órgãos de segurança pública

Apresentar, aplicado ao domínio do compartilhamento de sistemas de radiocomunicações entre órgãos de segurança pública, os seguintes resultados: os eventos de risco identificados; suas probabilidades e impactos ao ocorrerem; suas causas, efeitos e seus controles preventivos e reativos, além da Matriz de Riscos dos eventos de riscos identificados. A relevância caracteriza-se devido as diferentes organizações de segurança pública se comunicarem frequentemente com protocolos distintos. Como solução de melhor uso dos recursos, se propõe o compartilhamento entre sistemas de radiocomunicações de forças de segurança. No entanto, diante das incertezas dos resultados deste compartilhamento, a análise de riscos contribuirá para minimizar essas incertezas. Nesse cenário, busca-se identificar os eventos de riscos e seus elementos, afim de subsidiar à gestão na tomada de decisão para minimizar os riscos ora identificados. Pesquisa de natureza descritiva e qualitativa, onde o questionário foi passado por meio de formulários eletrônicos on-line entre os gestores de radiocomunicações do órgão em estudo, buscando atender aos objetivos da pesquisa. Foram identificados os eventos de risco, suas probabilidades de ocorrência e seus impactos na organização, posteriormente, diante de critérios técnicos, lançados na Matriz de Riscos, sinalizada em cores de acordo com a criticidade do risco. Ao final do estudo, após atendido os objetivos do estudo, foi possível apresentar uma Matriz de Riscos que auxilia na melhor visualização da criticidade dos eventos de riscos identificados. Os resultados se apresentam como uma ferramenta que podem auxiliar os gestores nas tomadas de decisões quando se pretende compartilhar sistemas de radiocomunicações.

Palavras-chave: Eventos de Risco; Efeitos de Risco; Fatores de Risco; Análise de Riscos; Compartilhamento de Sistemas de Radiocomunicações.

Identification of events, factors and effects of risks when sharing radiocommunication systems between public security bodies

To present, applied to the domain of radiocommunication systems sharing between public security agencies, the following results: the risk events identified; their probabilities and impacts when they occur; its causes, effects and preventive and reactive controls, in addition to the Risk Matrix of the identified risk events. Relevance is characterized by the fact that different public security organizations frequently communicate with different protocols. As a solution for better use of resources, it is proposed to share security forces between radiocommunication systems. However, in view of the uncertainties in the results of this sharing, the risk analysis will contribute to minimize these uncertainties. In this scenario, the aim is to identify risk events and their elements, in order to support management in decision making to minimize the risks now identified. Research of a descriptive and qualitative nature, where the questionnaire was passed through online electronic forms among the radiocommunication managers of the body under study, seeking to meet the research objectives. The risk events, their probabilities of occurrence and their impacts on the organization were identified, subsequently, in view of technical criteria, launched in the Risk Matrix, signaled in colors according to the criticality of the risk. At the end of the study, after meeting the objectives of the study, it was possible to present a Risk Matrix that helps to better visualize the criticality of the identified risk events. The results are presented as a tool that can assist managers in making decisions when they want to share radio systems.

Keywords: Risk Events; Risk Effects; Risk factors; Risk analysis; Sharing Radiocommunication Systems.

Topic: **Planejamento, Estratégia e Competitividade**

Reviewed anonymously in the process of blind peer.

Received: **09/10/2020**
Approved: **22/12/2020**

Aluisio Sardinha Garcia
Universidade Federal Rural do Rio de Janeiro, Brasil
http://lattes.cnpq.br/5500334588198072
http://orcid.org/0000-0002-0910-133X
aluisio.garcia@hotmail.com

André Luiz de Castro Leal
Universidade Federal Rural do Rio de Janeiro, Brasil
http://lattes.cnpq.br/7302692557217402
http://orcid.org/0000-0002-8206-0992
andrecastr@gmail.com

DOI: 10.6008/CBPC2179-684X.2020.004.0006

Referencing this:
GARCIA, A. S.; LEAL, A. L. C.. Identificação dos eventos, fatores e efeitos de risco ao compartilhar sistemas de radiocomunicações entre órgãos de segurança pública. **Revista Brasileira de Administração Científica**, v.11, n.4, p.79-91, 2020. DOI: http://doi.org/10.6008/CBPC2179-684X.2020.004.0006

INTRODUÇÃO

Assumpção et al. (2019), afirmam que: três diferentes tecnologias de sistemas de radiocomunicações são usadas na área de segurança no país, são elas o TETRA, o TETRAPOL e o APCO-25 e essas tecnologias não se comunicam, resultando na sobreposição de diferentes redes com coberturas similares que atendem aos diferentes órgãos que atuam na defesa e na segurança pública no país.

Freire et al. (2019) debatem a viabilidade de se compartilhar sistemas de radiocomunicações entre órgãos de segurança pública, onde se busca a otimização dos recursos, a unificação da gestão e os aspectos econômicos envolvidos.

Encontramos uma possível incerteza dos resultados do compartilhamento entre sistemas de radiocomunicações entre as organizações. Freire et al. (2019), afirmam a importância de se mitigar os riscos do compartilhamento, e relacionam, entre outras, as seguintes incertezas deste compartilhamento: se existe a disponibilidade do sistema para todas as organizações envolvidas; se são aplicados protocolos de prioridades de acesso ao sistema para operações integradas e se é possível garantir a disponibilidade ou restringir o acesso às informações, conforme a necessidade da informação trafegada.

Para Hoeflich et al. (2014) um *framework* funciona como um integrador de ferramentas de gestão de riscos. A proposição de um *framework* aplicado ao domínio do compartilhamento de sistemas de radiocomunicação, contribuirá para a viabilidade deste compartilhamento, identificando cenários de riscos em função dos eventos de riscos levantados na pesquisa de campo, seus efeitos de risco, os impactos e as probabilidades de ocorrência destes eventos de risco.

Os resultados apresentados neste artigo fazem parte da dissertação de mestrado do autor, cujo objetivo foi propor, aplicar e validar um *framework* de avaliação de riscos aplicado ao compartilhamento de sistemas de radiocomunicações entre órgãos de segurança pública, não havendo estudos similares publicados. Esta etapa foi de suma importância para as fases iniciais da pesquisa, pois se buscou envolver os especialistas do órgão no domínio de estudo para avaliar esses riscos antes que um método fosse proposto

Este artigo se propõe a trazer para a comunidade acadêmica, como foram identificados e apresentar: os eventos de riscos; as probabilidades de ocorrência dos eventos de risco identificados e os impactos que estes eventos causariam no objetivo de compartilhar sistemas de radiocomunicações entre forças de segurança pública na Organização de Estudo.

Também é objetivo deste artigo, apresentar os fatores de risco, os efeitos de riscos e o seus controles preventivos e reativos, parte importante da análise de riscos ao se compartilhar sistemas de radiocomunicações, contribuindo para minimizar as incertezas hoje encontradas, quando se avalia as possibilidades e consequências deste compartilhamento em estudo.

Para sua apresentação, o presente artigo está subdividido da seguinte forma: na seção 2, a Revisão Teórica; na seção 3, a Metodologia; na seção 4, os Resultados; na seção 5, a Discussão e na seção 6, as Conclusões.

REVISÃO TEÓRICA

Compartilhamento

Para Sundfeld (2006), pode ser entendido como o compartilhamento de sistemas de radiocomunicações a forma na qual se maximiza o uso de uma estrutura já existente, seu uso vai além do seu fim primário, a estrutura passa atender outras atividades de utilidade pública.

Laender (2002) e Escobar (2005) complementam ainda que o compartilhamento passa a existir quando existe o intuito de se diminuir custos, onde determinada estrutura que foi construída anteriormente para atendimento de um determinado serviço, 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.

Apesar de pouco conhecido, Nascimento (2013) afirma que para as organizações, o campo do compartilhamento de redes se mostra mais relevante com o passar do tempo, pois cada vez mais existe a necessidade das diferentes organizações se comunicarem entre si. No entanto, segundo Freire et al. (2019), para as redes de radiocomunicações de segurança, cada organização possui um sistema diferente de outras organizações e estes sistemas normalmente não se comunicam.

Sistemas de Radiocomunicações

Sistemas de telecomunicações, são sistemas que transmitem mensagens de um ponto para outro ponto, procurando preservar ao máximo a integridade do sinal transmitido. Para Tanenbaum (2003), são sistemas de comunicações, sistemas que fazem uso de sinais elétricos na transmissão/recepção de informações, estes sistemas estão divididos em dois grupos: sistemas que se utilizam de cabos e sistemas que não fazem uso de fio (sistemas sem fio), neste último estão incluídas as transmissões via rádio, as radiocomunicações.

Ainda, segundo Tanenbaum (2003), um sistema via rádio dispensa o meio físico e utiliza ondas eletromagnéticas como elemento de ligação entre emissor e receptor.

Existem três principais padrões de sistemas de radiocomunicação digitais usados na segurança pública no Brasil, cada um com as suas vantagens e desvantagens, foram desenvolvidos para disponibilizar recursos e serviços para atender a demanda de comunicação digital na área de segurança, com algo em comum: as tecnologias não se conectam (AMARAL, 2010).

Esses três principais padrões de sistemas de radiocomunicações digitais usados na área de segurança no Brasil são: o APCO-25; o TETRA e o TETRAPOL.

O padrão APCO-25, 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). Possui como fornecedor a Motorola, no Brasil foi absorvido na sua maioria pelo Exército Brasileiro (EB), no campo civil, pela Secretaria de Segurança Pública (SESP) do Estado de São Paulo.

O padrão TETRAPOL tem sua origem na França, possui suas especificações segundo as normas do Instituto de Padronização de Telecomunicações Europeu (ETSI) (TETRAPOL, 2011). Seu fornecedor é o grupo

Airbus, no Brasil possui sua maior rede instalada na Polícia Federal, por meio de uma rede nacional, possui cobertura em todos os estados e possui instalada também uma rede instalada na SESP do Ceará.

O padrão TETRA possui a sua base na padronização do ETSI, onde inúmeras empresas fabricam e comercializam o padrão. Seu protocolo foi pensado para usos governamentais em Segurança Pública, diferentemente dos padrões anteriores, APCO 25 e TETRAPOL, não possuem desenvolvedor proprietário, devido a isso, o padrão 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 e diversas secretarias de segurança Pública no Brasil, como a do Estado do Rio de Janeiro, da Bahia, do Distrito Federal.

Riscos

No PMBOK (2017), os riscos se apresentam como acontecimentos ou condições futuras, que podem provocar impacto em um projeto ou organização. Já para o APM (2013), o risco é um evento ou condição incerta, ao ocorrer, poderá ter um efeito positivo ou negativo sobre um ou mais objetivos do projeto.

Rabechini et al. (2012) teorizam que a verificação do risco é considerada uma das mais importantes tarefas de gerenciamento de projetos, para Russo et al. (2014), esta etapa trata de questões para antecipação e minimização dos eventos que possam impactar negativamente nos objetivos do projeto.

Ainda o PMBOK (2017) destaca que um risco pode ter uma ou várias causas com os mais diversos impactos. Ao ocorrer um risco, este pode causar impacto no custo, no cronograma ou desempenho de um projeto. Os riscos podem ocorrer sob a forma de oportunidades ou ameaças ao projeto. Ao estudar os riscos ao projeto, devem se considerar estratégias que visem potencializar os resultados positivos e minimizar as consequências geradas pelos eventos negativos (PMBOK, 2017).

Matriz de Riscos

O PMBOK (2017) ressalta a importância da Matriz de Riscos para os gestores que trabalham em mensurar, avaliar e ordenar os eventos de risco de uma forma com uma fácil visualização dos eventos de riscos que podem afetar a busca de se atingir os objetivos do processo. Já na CGU (2018), na Matriz de Riscos são mensurados os níveis de riscos identificados na etapa de avaliação dos riscos, e realiza-se um estudo de interação entre os valores de probabilidade e impacto, por meio do produto entre esses valores, resultando na formação da Matriz de Riscos.

Para a CGU (2018), na Matriz de Riscos é possível classificar os riscos de forma rápida e direta, permite uma resposta/ação a estes riscos, visando proteger os objetivos principais do projeto. Ainda segundo a CGU (2018), a Matriz de Riscos possui seus elementos com as quatro classificações, são elas: RE – Risco Extremo; RA – Risco Alto; RM – Risco Médio e RB - Risco Baixo.

METODOLOGIA

Aspectos Metodológicos

De abordagem qualitativa e descritiva, os respondentes somente seguiam com a pesquisa ao concordarem com o TCLE (Termo de Consentimento Livre e Esclarecido) apresentado antes das perguntas do formulário. No TCLE disponibilizado aos respondentes, onde os respondentes ao concordarem com o TCLE da pesquisa seguiam com a pesquisa e caso não concordassem eram direcionados para uma página onde finalizava a pesquisa.

Como critério para participarem da pesquisa, os participantes eram, na época da pesquisa, gestores da rede de radiocomunicações dos setores de tecnologia da informação dos estados e dos setores de telecomunicações em Brasília do órgão em estudo de segurança pública. Foram excluídos servidores que estão na área de radiocomunicações há menos de um ano no órgão.

A pesquisa foi disponibilizada para 54 servidores dos 26 estados mais o Distrito Federal, no entanto, obtivemos 51 respostas de 25 estados mais o Distrito Federal.

Todos os gestores que concordaram em participar da pesquisa, ao darem o aceite no Termo de Consentimento Livre e Esclarecido, 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 foi dito e do anonimato de cada respondente.

Obtenção de Dados

A obtenção dos dados ocorreu por meio de um questionário formulário on-line. Na primeira pergunta foi disponibilizada uma lista de eventos de riscos. 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.

A segunda pergunta respondida no formulário procurou levantar a probabilidade de ocorrência dos eventos de riscos indicados na pergunta anterior, para isso, 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.

A tela do formulário com parte da segunda pergunta, como exemplo são apresentados os três primeiros eventos de risco da lista, onde somente era possível prosseguir com o formulário se o respondente indicasse uma das probabilidades disponibilizadas para cada fator de risco.

A terceira pergunta respondida no formulário, procurou levantar o impacto para a ocorrência dos riscos indicados na lista disponibilizada na primeira pergunta, para isso, por meio de uma lista de eventos de risco, os respondentes indicavam uma graduação para o impacto na 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.

Na tela do formulário para parte da terceira pergunta, como exemplo, os três primeiros eventos de riscos da lista, onde somente era possível o respondente prosseguir com o preenchimento do formulário se indicasse um dos impactos disponibilizados para cada fator de risco.

RESULTADOS

Identificação dos Eventos de Risco.

Ao fim da pesquisa de campo foram identificados os 21 eventos de riscos listados no Quadro 1, pela característica colaborativa do formulário, os eventos de risco foram identificados pelo pesquisador, na etapa de elaboração do formulário, pelos respondentes, na etapa de calibragem ou durante a pesquisa disponibilizada a todos os respondentes.

Quadro 1: Eventos de risco.

1 - A rede não suportar o tráfego de novos usuários da Organização de Estudo.
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 Organização de Estudo não adquirir os equipamentos/acessórios necessários para o uso da nova rede.
8 - A cobertura da nova rede não atender à necessidade de cobertura da Organização de Estudo.
9 - A Organização de Estudo 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 Organização de Estudo.
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.

A Figura 1 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.

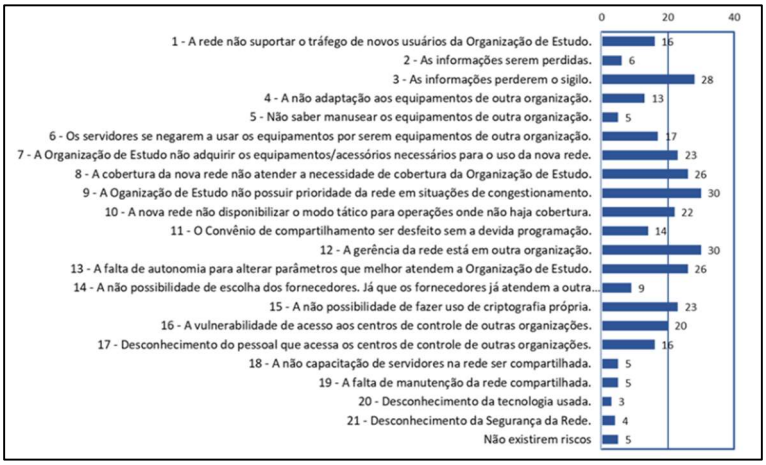

Figura 1: Indicação dos Eventos de Risco pelos respondentes na pesquisa de campo.

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

No Quadro 2 foram listados para cada evento de risco os fatores de risco, os efeitos de risco, seus controles preventivos e seus controles reativos.

Para a maior relevância do 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 1 deste artigo.

Quadro 2: Identificação dos fatores e efeito de risco e seus controles.

Evento de Risco 1 - A rede não suportar o tráfego de novos usuários da Organização de Estudo.			
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.	Reati	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.	Preventi	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.	Reati	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.	Reati	Realizar treinamento nos novos equipamentos.
Evento de Risco 7 - A Organização de Estudo 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 Organização de Estudo.			
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 Organização de Estudo 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.	Preventi	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.	Reati	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 Organização e Estudoi não adquirir o sistema tático.	Preventi	Buscar um sistema de contingencias que supra o modo tático Realizar estudos para a compra do sistema tático.
Ef	Falta de cobertura em áreas remotas.	Re	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 contratais 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.	Reati	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.	Preventi	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.	Reati	Buscar junto à organização que possui a gerencia da rede as possibilidades de customizar a rede para que melhor possa atender a Organização de Estudo.
Evento de Risco 13 - A falta de autonomia para alterar parâmetros que melhor atendem a Organização de Estudo.			
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 Organização de Estudo.	Preventivo	Buscar junto à organização que gerencia a rede acesso aos controles da rede. Buscar instruir cláusulas no contrato de compartilhamento que permitam a Organização de Estudo 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 Organização de Estudo. 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 Organização de Estudo não possuir interesse em ter uma rede própria.	Preventi	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 Organização de Estudo. O sistema não possibilitar instalar criptografia própria.	Preventivo	Buscar junto à organização que gerencia o sistema a possibilidade de instalar uma criptografia própria da Organização de Estudo. Buscar junto à organização que gerencia o sistema instalar na Organização de Estudo 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 Organização de Estudo 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 Organização de Estudo. 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.	Reati	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 Organização de Estudo.	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.	Reati	Procurar fazer uso de códigos na comunicação.

Elaboração da Matriz de Riscos

Para a elaboração da Matriz de Riscos, recorremos a avaliação de riscos da Metodologia de Gerenciamento de Riscos da CGU (2018). Os elementos da Matriz de Riscos são os resultados do produto do valor do peso definido para probabilidade pelo valor do peso definido para o Impacto. A escala de probabilidade toma como base a Tabela 1, onde se mesura a probabilidade desde muito baixa até muito alta com seus pesos de 1 a 10.

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. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	10

Fonte: Extraída da Metodologia de Gestão de Riscos da CGU (2018).

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).

Para a escala de impacto, se toma como base a Tabela 2 onde também é mensurado o impacto desde muito baixo até muito alto com seus pesos de 1 a 10.

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.

$$RI = NP \times NI$$

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.

Na matriz de riscos é possível observar um código de cores para o resultado do produto da probabilidade pelo impacto, onde para este resultado temos 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.

Tabela 3: Classificação do Risco.

Classificação	Faixa
Risco Baixo - RB	0 – 9,99
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).

Os eventos de risco são inseridos então com o seu código correspondente (Evento de Risco - ERn), onde n corresponde ao código dado ao evento de risco de 1 a 21 na matriz de risco, onde será possível uma melhor visualização dos riscos que merecem um tratamento prioritário como apresentado na Figura 2.

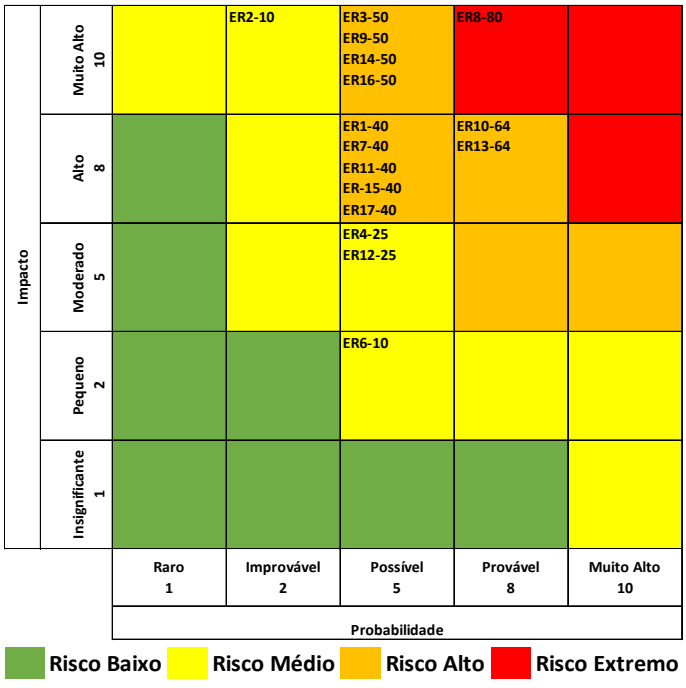

Figura 2: Matriz de Riscos.

DISCUSSÃO

Como apresentado no Quadro 1, foram identificados 21 eventos de risco, os eventos de risco com maior indicação pelos respondentes foram os eventos de risco 9 e 12 (a Organização de Estudo 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.

Era 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, suas consequências.

Para cada evento de risco identificado, primeiramente foi identificado os fatores de risco, ou seja, as causas para que este evento de risco ocorresse, foram identificados então os efeitos de risco, as consequências caso esses eventos de riscos viessem a ocorrer, por fim foram identificados os seus controles, os preventivos e reativos, os primeiros eram os controles que eram aplicados antes dos eventos de risco ocorrerem, contribuíam para que os eventos de risco não ocorressem, já os controles reativos eram aplicados após os eventos de riscos ocorrerem com o intuito de minimizar os efeitos dos eventos de riscos ao ocorrerem.

A próxima etapa foi construir a Matiz de Riscos, ela possui como ponto forte seu grande poder de comunicação visual que é potencializado por meio do seu código de cores, no seu eixo vertical é apresentada a escala de impacto e no seu eixo horizontal é apresentada a escala de probabilidade.

Os eventos de riscos localizados na região verde, são riscos classificados em riscos baixos, estes recebem menor ação de mitigação, por se classificarem em riscos que podem trazer menores prejuízos para a organização no objetivo a ser alcançado. No estudo não foram encontrados Riscos Baixos (RB).

Já os riscos médios, identificados na cor amarela, 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. No estudo, os Eventos de Risco 2, 4, 6 e 12, obtiveram como resultado do produto da Probabilidade x Impacto o nível de Risco Médio (RM) conforme a Tabela 3, os eventos de risco classificados como RM sofrem menor monitoramento que os riscos altos e maior monitoramento que os riscos baixos, devem ser observados pois podem possuir impactos que prejudiquem os objetivos do projeto.

Já os riscos altos, apresentados na Matriz de Risco na cor laranja, devem ser monitorados com frequência, pois se não mitigados podem resultar em efeitos tão grandes quanto os riscos extremos. Para o estudo, os Eventos de Risco 1, 3, 7, 9, 10, 11, 13, 14, 15, 16 e 17 obtiveram como resultado do produto da Probabilidade x Impacto o nível de Risco Alto (RA) conforme a Tabela 3, os eventos de risco classificados como RA devem ser monitorados com frequência, pois se não mitigados podem resultar em efeitos tão grandes quanto os riscos extremos.

Os eventos de risco localizados na Matriz de Risco na região vermelha, ou seja, de Riscos Extremo (RE), devem receber tratamento prioritário. Para o estudo o Evento de Risco 8 obteve como resultado do

produto da Probabilidade x Impacto o nível de Risco Extremo (RE) conforme a Tabela 3, os eventos de risco classificados como RE, apresentam riscos com alto impacto e alta probabilidade de ocorrência, nenhum projeto sobrevive com riscos em nível tão alto a longo prazo, são necessárias ações de mitigação para que o projeto sobreviva.

CONCLUSÕES

A expertise dos servidores envolvidos e a participação de quase 100% das unidades contribuíram para a relevância e ratificam os resultados obtidos na pesquisa, retornando resultados mais próximos da realidade considerando os diferentes contextos e realidades no qual estão inseridos os especialistas da Organização de Estudo nos mais diversos estados.

Foi apresentada a Matriz de Riscos, um conjunto de informações onde os resultados dos níveis de risco dos eventos de risco identificados, são apresentados de forma intuitiva, por meio de um código de cores que facilita a visualização da criticidade dos eventos de risco estudados, destacando os eventos de risco que devem receber ações de mitigação prioritárias para o atendimento do objetivo de compartilhar redes de radiocomunicações.

O conjunto de informações reunidas na pesquisa, acerca do universo estudado, irão contribuir para tornar o 'terreno' do compartilhamento entre sistemas de radiocomunicações mais conhecido, facilitando e fomentando essa cultura entre forças de segurança, essas informações ainda auxiliam na elaboração de processos específicos de análise de riscos destes compartilhamentos e são importante parte de um objetivo maior da definição da arquitetura de um *framework* de avaliação de riscos.

O compartilhamento de estruturas de comunicações entre órgãos de segurança pública cumpre um importante papel ligado a sustentabilidade ao otimizar a aplicação dos recursos disponibilizados pelo poder público, contribuindo dessa forma para reduzir as diversas redes sobrepostas e os diversos recursos necessários para a instalação de uma rede de radiocomunicações de segurança pública, além de se destacar tecnicamente por retornar melhores resultados em operações integradas, já que ao compartilharem um mesmo sistema, as organizações ganham facilidades para se comunicarem entre si.

REFERÊNCIAS

AMARAL, C. T.. **Rede de rádio digital de segurança pública:** estudo de caso para a copa do mundo de futebol em Belo Horizonte. Monografia (Especialização) - Centro Universitário de Belo Horizonte, Belo Horizonte, 2010.

APM. Association for Project Management. **APM Body of Knowledge**. 6 ed. London: Association for Project Management, 2013.

ASSUMPÇÃO, L.; MINGHELLI, M.. **Aproximação entre a Ciência da Informação com a Ciência Policial**. Florianópolis: SENAC, 2019.

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, v.6, n.25, p.181-212, 2006.
DOI: http://dx.doi.org/10.21056/aec.v6i25.433

CGU. Controladoria-Geral da União. **Metodologia de Gestão de Riscos**. Brasília: MTCGU, 2018.

ESCOBAR, J. C.. **Serviços de telecomunicações**: aspectos jurídicos e regulatórios. Porto Alegre: Livraria do Advogado, 2005.

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

FREIRE, D. V. C.; JORGE, J. M. R.; CANDIDO, A. C.. **Aproximação entre a ciência da informação com a ciência policial**. Florianópolis: SENAC, 2019.

HOEFLICH, S. L.; BLOS, M. F.; FIGUEIREDO, A. E. P.; DIAS, E. M.. Proposta de framework de gerenciamento de riscos orgânicos aplicado à logística. In: SIMPÓSIO DE PESQUISA OPERACIONAL E LOGÍSTICA DA MARINHA - SPOLM 2014, 17. **Anais.** São Paulo: Blucher, 2014. p.522-533. **DOI:** http://doi.org/10.5151/marine-spolm2014-126503.

LAENDER, G. B.. Interconexão, Unbundling e Compartilhamento de Meios de Rede de Telecomunicação. **Revista de Informação Legislativa**, Brasília, v.39, n.154, 2002.

MOTOROLA, L. F.. Curso. **Conceitos Trunking**. Campinas, 2010.

NASCIMENTO, M. G. O.. A Atuação Preventiva da Anatel na Promoção da Concorrência no Mercado Brasileiro de Telecomunicações e o Plano Geral de Metas de Competição. **Revista Publicações da Escola da AGU – O Direito nas Telecomunicações**, Brasília, v.5, n.24, 2013.

PMBOK. Project Management Institute. **Guia PMBOK**: um guia para o conjunto de conhecimentos em gerenciamento de projetos. 6 ed. Harrisburg: PMI, 2017.

RABECHINI JUNIOR, R.; CARVALHO, M. M.. Relacionamento entre gerenciamento de risco e sucesso de projetos. **Production,** São Paulo, v.23, n.3, p.570-581, 2012. **DOI:** http://doi.org/10.1590/S0103-65132012005000091

RUSSO, R. F. S. M.; SBRAGIA R.. Incerteza imprevisível em projetos inovadores: criando sentido com a gestão de projetos 2012. **Revista de Gestão e Projetos**, São Paulo, v.5, n.2, 2014. **DOI:** http://doi.org/10.5585/gep.v5i2.204.

SUNDFELD, C. A.. Estudo jurídico sobre o preço do compartilhamento de infraestrutura de energia elétrica. **Revista Eletrônica de Direito Administrativo Econômico**, Salvador, v.4, 2006.

TANENBAUM, A. S.. **Redes de computadores**. São Paulo: São Paulo, 2003.

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