Área Temática:

TECNOLOGIA, INTELIGÊNCIA ARTIFICIAL E TRANSFORMAÇÃO DIGITAL EM ADMINISTRAÇÃO

INFRAESTRUTURA CRÍTICA SOB AMEAÇA: RISCOS DE NEGÓCIO PARA A SEGURANÇA CIBERNÉTICA EM SISTEMAS DE TRANSPORTE METROPOLITANO

Resumo: As infraestruturas críticas constituem elementos indispensáveis ao funcionamento da sociedade contemporânea, mas a crescente digitalização tem ampliado sua vulnerabilidade a ameaças cibernéticas. Entre essas infraestruturas, os sistemas de transporte metroviário ocupam posição central na mobilidade urbana e, consequentemente, tornam-se alvos estratégicos para agentes maliciosos. Este estudo teve como objetivo identificar e analisar os principais riscos de negócio associados à operação de metrôs, cujas origens estão relacionadas a incidentes de segurança cibernética. Para tanto, foi conduzida uma pesquisa de natureza aplicada e caráter exploratório, apoiada em revisão bibliográfica e na análise de reportagens sobre ataques cibernéticos a companhias metroviárias. A metodologia integrou a Análise Preliminar de Perigos (APP), a técnica Bow Tie e o framework CIS Controls v8, permitindo sistematizar riscos, causas, consequências e controles de mitigação. Os resultados apontaram sete riscos de negócio, 27 possíveis causas e 10 potenciais consequências, destacando-se vulnerabilidades relacionadas ao vazamento de dados pessoais e internos, indisponibilidade de sistemas de bilhetagem e descumprimento de normas legais. Constatou-se que a aplicação de controles específicos, como os do CIS v8, apresenta elevada eficácia para reduzir impactos, inclusive otimizando recursos ao mitigar múltiplos riscos com ações convergentes. Como contribuição, o trabalho amplia a compreensão dos efeitos organizacionais e sociais da materialização de ataques cibernéticos em transportes metropolitanos, fornece evidências sobre a necessidade de gestão integrada de riscos no setor e subsidia gestores públicos e privados na formulação de estratégias de resiliência e continuidade operacional.

Palavras-chave: resiliência cibernética; continuidade operacional; segurança na mobilidade urbana; gestão de riscos; proteção de infraestrutura de transporte.

Abstract: Critical infrastructures are indispensable elements for the functioning of contemporary society, but increasing digitalization has amplified their vulnerability to cyber threats. Among these infrastructures, metro transportation systems play a central role in urban mobility and, consequently, become strategic targets for malicious actors. This study aimed to identify and analyze the main business risks associated with metro operations originating from cybersecurity incidents. To achieve this, an applied and exploratory research was conducted, supported by a literature review and an analysis of news reports on cyberattacks against metro companies. The methodology integrated the Preliminary Hazard Analysis (PHA), the Bow Tie technique, and the CIS Controls v8 framework, enabling the systematization of risks, causes, consequences, and mitigation controls. The results revealed seven business risks, 27 possible causes, and 10 potential consequences, with particular emphasis on vulnerabilities related to the leakage of personal and internal data,

unavailability of ticketing systems, and non-compliance with legal regulations. The findings indicated that applying specific controls, such as those from CIS v8, is highly effective in reducing impacts, optimizing resources by mitigating multiple risks through convergent actions. As a contribution, this study enhances the understanding of organizational and social effects of cyberattacks on metropolitan transportation, provides evidence of the need for integrated risk management in the sector, and supports public and private managers in formulating resilience and business continuity strategies.

Keywords: cyber resilience; business continuity; metro transportation; risk management; critical infrastructure.

1. INTRODUÇÃO

A sociedade contemporânea atualmente opera com base em uma complexa rede de infraestruturas críticas (ICs) as quais são indispensáveis para o funcionamento, sobrevivência e desenvolvimento. As ICs compreendem instalações, serviços e bens essenciais, como abastecimento de água, energia, transportes, cuja interrupção ou destruição pode provocar impactos de ordem social, econômica ou comprometer a segurança do Estado e da sociedade (Brasil, 2022; Da Silva et al, 2025; Lima et al., 2022).

Com o avanço da transformação digital, as infraestruturas críticas tornaram-se ainda mais dependentes de tecnologias. Impõe-se, assim, à Administração Pública a modernização de seus métodos e ferramentas de trabalho, principalmente os ligados ao uso de tecnologias da informação (Moura, 2016). No entanto, operar em um ambiente cada vez mais interconectado impõe dificuldades adicionais, sobretudo na proteção de dados sensíveis. Além disso, é necessário que cumpram suas funções institucionais em conformidade com as diretrizes estabelecidas pelos órgãos centrais do governo (Dzazali e Hussein, 2021).

A inserção de tecnologias nas IC eleva sua capacidade operacional, garantindo serviços essenciais com mais inteligência e agilidade. Contudo, juntamente com os benefícios introduzidos pelo uso da tecnologia, também surgem novos fatores de risco (Moreira et al., 2021). Nesse contexto, quando as IC se tornam alvos de ataques cibernéticos, os danos podem se manifestar na interrupção ou degradação dos serviços prestados, afetando diretamente a população e, em muitos casos, gerando efeitos em cascata sobre outras ICs interdependentes (Machado, 2020).

Nesse sentido, os riscos são definidos como os efeitos das incertezas sobre os objetivos, exigindo uma identificação e análise adequadas para sua mitigação (ABNT, 2018). O gerenciamento de riscos configura-se como um processo estratégico para organizações, uma vez que considera os contextos internos e externos da instituição, abrangendo fatores humanos, culturais, sociais e econômicos que possam afetar sua estabilidade operacional (IPQ, 2018).

Diante da limitação de pesquisas correlatas que abordem de forma específica os riscos no setor metroviário, este estudo tem como objetivo identificar os principais riscos de negócio no funcionamento dos metrôs, cujas causas têm como origem o risco cibernético. Para isso, serão utilizados o método *Bow Tie*, que permite a visualização das causas, consequências e barreiras associadas aos riscos, e o framework de controles CIS Controls v8, que oferece diretrizes reconhecidas internacionalmente para a implementação de medidas de segurança cibernética.

Este trabalho está estruturado da seguinte forma: a seção 2 apresenta os principais conceitos abordados na literatura sobre o tema; a seção 3 descreve a metodologia adotada para a identificação dos riscos de negócio; a seção 4 expõe os riscos de negócio identificados nas companhias metroferroviárias e analisa os resultados obtidos; por fim, a seção 5 discorre sobre as limitações do estudo, propõe direções para pesquisas futuras e apresenta as considerações finais.

2. FUNDAMENTAÇÃO TEÓRICA

Esta seção introduz os conceitos para compreensão do estudo, abordando Risco, Gestão de Riscos e Infraestrutura Crítica, as atividades das empresas metroviárias e trabalhos relacionados à pesquisa.

2.1. Risco, Gestão de Riscos

No âmbito organizacional, as incertezas ocorrem a todo momento. Uma incerteza refere-se a situações em que não há informações suficientes para o entendimento do cenário ou conhecimento quanto às consequências de determinado evento (Bermejo et al., 2018). Nesse contexto, Barragan et al. (2006) definem o risco como a possibilidade de ocorrência de um evento futuro não previsto, podendo gerar consequências positivas ou negativas ao objetivo almejado.

A gestão de riscos refere-se à noção de que eventos incertos podem acontecer e gerar prejuízos para as organizações. Portanto, a administração dos riscos fornece aos gestores o conhecimento de quais riscos as empresas estão expostas (Fernandes et al., 2014). Na medida em que todas as atividades organizacionais envolvem riscos, os gestores devem atentar-se para esses fenômenos, dado que existe a possibilidade do sucesso ou do fracasso em determinadas decisões. Logo, compete aos administradores avaliarem e mensurarem os riscos envolvidos, administrando-os com o intuito de reduzir as consequências indesejadas ou maximizar a possibilidade dos eventos desejados (Bergamini Junior, 2005). Esse processo tem grande relevância e deve ser realizado e revisado periodicamente (Relim et al., 2020).

2.2. Infraestrutura Crítica

As infraestruturas críticas (IC), segundo o Glossário de Segurança da Informação, são definidas como instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, podem causar sérios impactos social, econômico, político, internacional ou à segurança (Brasil, 2021). Esse conceito evidencia a relevância estratégica das ICs, uma vez que sua operação contínua sustenta setores vitais, tornando-se alvos sensíveis a diversos tipos de ataques.

Diante dessa vulnerabilidade, a Política Nacional de Inteligência (PNI) destaca que os ataques consistem em ações deliberadas que utilizam recursos de tecnologia da informação e comunicação com o objetivo de interromper, penetrar, adulterar ou destruir redes críticas utilizadas por setores públicos e privados essenciais para o funcionamento do país, incluindo aquelas pertencentes à infraestrutura crítica nacional (Brasil, 2020). A implementação de estratégias de segurança cibernética, alinhadas à normativas e diretrizes internacionais, é fundamental para mitigar riscos e garantir a continuidade das operações (Carvalho, 2011).

2.3. Atividades Principais

O metrô é um sistema ferroviário subterrâneo usado para transportar grandes quantidades de passageiros em áreas urbanas e suburbanas (Encyclopaedia Britannica, 2025). Caracterizado por alta velocidade, alta capacidade e alto nível de segurança, os sistemas de metrô atendem às necessidades de

mobilidade das pessoas de forma econômica e ecologicamente eficiente há mais de um século e meio (Lin et al., 2024).

No que diz respeito aos aspectos sociais, o metrô simboliza, por comparação, um conjunto de atividades e de elementos fixos, como os deslocamentos realizados pelos usuários que fazem uso do sistema, criando conexões entre os diferentes pontos da rede de metrô e promovendo uma variedade de interações espaciais (Corrêa, 1997). Operando geralmente como um bem estatal, mas muitas vezes com gestão terceirizada por meio de parcerias público-privadas (Freitas, 2023).

2.4. Trabalhos Correlatos

Diversos estudos têm abordado a questão da segurança em infraestruturas críticas sob diferentes perspectivas. Ferreira (2020) discute a crescente vulnerabilidade desses sistemas diante de ameaças modernas, destacando a necessidade de resiliência como eixo central. Silva (2015), por sua vez, aprofunda o debate sobre cibersegurança nacional, ressaltando a importância de políticas públicas e estratégias integradas para proteger setores essenciais. Junior et al. (2023) analisam a gestão de riscos no setor público, enfatizando métodos e práticas aplicáveis à proteção de ativos críticos governamentais, em linha com os desafios apontados nos estudos anteriores. Em conjunto, esses trabalhos evidenciam um panorama abrangente na proteção de infraestruturas críticas no Brasil.

No cenário internacional, Malatji, Marnewick e Von Solms (2022) propõem um modelo de capacidades de segurança cibernética voltado à resiliência de infraestruturas críticas, conceito que dialoga com os princípios de gestão abordados nos trabalhos nacionais. Já Tonn et al. (2019) discutem a aplicação de seguros cibernéticos no setor de transporte, apontando lacunas ao questionar se os riscos de segurança cibernética no transporte estão sendo devidamente priorizados. Complementando essa abordagem setorial, Kour, Karim e Thaduri (2020) propõem um modelo de maturidade em segurança cibernética para ferrovias.

3. METODOLOGIA

Este estudo caracteriza-se como uma pesquisa de natureza aplicada, uma vez que busca a aplicação prática do conhecimento e a solução de problemas reais. Adotou-se o método qualitativo para analisar o fenômeno em profundidade, captando seus aspectos subjetivos e não mensuráveis, cuja análise não pode ser limitada a dados numéricos (Silva e Menezes, 2005, p. 20).

A pesquisa possui caráter exploratório, pois busca ampliar o conhecimento do pesquisador sobre determinado fenômeno, favorecer a formulação de hipóteses, bem como permitir o aprimoramento e a clarificação de conceitos, contribuindo para estudos futuros mais precisos (Lakatos e Marconi, 1985, p. 86). Tal característica evidencia a flexibilidade e a profundidade desse tipo de estudo, especialmente em contextos nos quais há pouca familiaridade com o objeto ou ausência de referenciais consolidados (Fernandes e Gomes, 2003). A Figura 1 demonstra as etapas decorridas neste trabalho.

Figura 1. Etapas da pesquisa

Para uma análise mais abrangente dos riscos cibernéticos, esta pesquisa adota uma abordagem metodológica integrada, combinando três ferramentas: a Análise Preliminar de Perigos (APP), a metodologia *Bow Tie* e o *framework* CIS Controls V8.

A Análise Preliminar de Riscos (APR), também conhecida como Análise Preliminar de Perigos (APP), refere-se de um método de natureza qualitativa, utilizado nas etapas iniciais de desenvolvimento de um sistema, especialmente quando ainda há informações limitadas disponíveis, com a finalidade de identificar os potenciais riscos que podem surgir ao longo do processo (Pardo, 2009). A APP é um método de análise simples que busca identificar perigos, situações e eventos potencialmente perigosos que possam representar riscos a uma determinada atividade, instalação ou sistema (ABNT, 2012, p. 29). A análise preliminar de perigos foi realizada com base em reportagens de casos reais de ataques cibernéticos a companhias metroviárias.

O *Bow Tie* trata-se da construção de um diagrama, amplamente utilizado na gestão de riscos por facilitar a compreensão de cenários complexos. Sua simplicidade está ligada ao propósito da metodologia, que é apresentar de forma acessível, mesmo para não especialistas, as interações entre causas e os efeitos de um evento que perdeu o controle (CCPS, 2018). A técnica é especialmente eficaz em situações nas quais um único evento pode ser originado por diferentes causas e resultar em variadas consequências ABNT (2012). Nessa metodologia são mapeadas as causas, consequências, barreiras de prevenção, barreiras mitigadoras, além dos fatores e controles de degradação (CCPS, 2018).

A escolha do *framework* CIS Controls versão 8 (CIS V8) nesta pesquisa se justifica por sua abordagem prática, estruturada e amplamente reconhecida no campo da segurança da informação. O CIS é uma organização sem fins lucrativos cuja missão é identificar, desenvolver, validar e promover boas práticas voltadas à defesa cibernética (Microsoft, 2023). De acordo com o GAT (2022), os CIS Controls V8 consistem em um conjunto prescritivo e prioritário de ações de segurança cibernética, organizadas para mitigar os ataques mais comuns e críticos. Este framework oferece suporte à conformidade em um cenário onde coexistem múltiplas estruturas regulatórias e normativas. Atualmente, o CIS V8 é composto por 18 controles principais, os quais são desdobrados em 156 salvaguardas específicas. Segundo GAT (2022), cada controle possui um escopo abrangente, porém estruturado com base em princípios sólidos de segurança.

4. RESULTADOS E DISCUSSÃO

A partir da análise preliminar de perigos, realizada com base em notícias e reportagens divulgados na mídia especializada sobre ataques cibernéticos a

sistemas de companhias metroviárias, elaborou-se a Tabela 1, que cataloga os ataques em ordem de 2016 até 2024.

Tabela 1. Reportagens analisadas

Evento	Descrição Resumida
Ataque ao metrô de São Francisco (EUA) - 2016	Sistema interno/bilhetagem inoperante, roubo de dados
Ataque ao Metrô de Kiev (Ucrânia) - 2017	Sistema interno/bilhetagem inoperante
Ataque ao metrô da (Dinamarca)-2018	Paralisação de sistemas internos.
Ataque a ferrovia do (Irã)- 2021	Portais foram derrubados e divulgaram alertas falsos.
Ataque a CPTM de (São Paulo) – 2022	Vazamento de documentos internos e dados sigilosos na deep web.
Ataque ao metrô de São Paulo- 2023	Vazamento de dados de 13 milhões de usuários (CPF, RG, senhas).
Ataque ao metrô de Washington - 2024	O site do metrô ficou inacessível por 2 horas.

Fonte: Elaborado pelos autores (2025)

Foram inicialmente listados 22 riscos potenciais, sendo organizados com a técnica *Bow Tie*. Observou-se que parte dos riscos iniciais representava, na verdade, causas ou consequências de eventos maiores, havendo ainda casos de repetição. Essa etapa de verificação e categorização foi essencial para consolidar os resultados.

Ao final da análise foram consolidados 7 riscos de negócio, 27 possíveis causas e 10 possíveis consequências. Na Tabela 2 são apresentados os riscos de negócios.

Tabela 2. Risco de negócio em companhias metroviárias

[1] Vazamento de dados pessoais de usuários (ex: CPF, RG, senhas)
[2] Indisponibilidade de sistemas de bilhetagem
[3] Interrupção de serviços digitais (ex: sites, aplicativos, portais)
[4] Vazamento de documentos internos e dados sensíveis
[5] Descumprimento de normas legais e regulatórias (ex: LGPD)
[6] Manipulação de informações operacionais (ex: falsos avisos de atraso)
[7] Perda de informações administrativas críticas

Fonte: Elaborado pelos autores (2025)

A análise *Bow Tie* foi utilizada para compreender como diferentes causas podem levar aos riscos de negócio identificados. A Tabela 3 mostra essas causas agrupadas por tipo de risco.

Tabela 3. Análise *Bow Tie* (Fontes e Riscos de Negócio)

Causas e Fontes	Riscos
Ataque cibernético Falhas de segurança em sistemas Falhas na gestão de credenciais Falta de monitoramento Sabotagem por parte de usuários ou funcionários internos Falta de treinamentos sobre sistemas de informação	[1][4]
Ataque cibernético e exploração Erros humanos ou falhas operacionais Falha na infraestrutura de TI Ausência de controle de acesso privilegiado Sabotagem por parte de usuários ou funcionários internos Sistemas sem manutenção e ausência de criptografia Falta de padronização e procedimentos	[2][3][7]
Falta de conhecimento/capacitação sobre as legislações Processos de compliance inadequados Excesso de privilégio Falta de auditoria contínua sobre processos Documentações/normas internas desatualizadas Ausência de recursos dedicados à conformidade legal Dificuldade na compreensão e aplicação prática dos requisitos legais	[5]
Ataque cibernético e exploração Privilégios excessivos e falta de segregação Vulnerabilidades em software ou servidor Sistemas sem manutenção e criptografia Sabotagem por parte dos usuários ou funcionários internos Acesso indevido Falta de treinamentos sobre sistemas de informação	[6]

Fonte: Elaborado pelos autores (2025)

A Tabela 4 reúne de forma organizada todas possíveis consequências dos riscos de negócio.

Tabela 4. Análise *Bow Tie* (Consequências dos Riscos)

Consequências	Riscos de Negócio
Prejuízo à imagem e credibilidade	[1][2][3][4][5][6][7]
Exposição de dados sensíveis	[1][4][5]
Custo de recuperação de dados/treinamento	[3][7]
Danos financeiros a administração pública	[2][7]
Correção de processos administrativos	[5][7]

Invalidação de documentos	[7]
Processos Judiciais/indenização/Multa	[1][4][5]
Golpes contra afetados da exposição	[1][4]
Interrupção de serviços	[2][3][5][7]
Insatisfação dos usuários	[2][3][5][6]

Fonte: Elaborado pelos autores (2025)

A partir da análise das consequências é possível compreender que mesmo com medidas de segurança implementadas, os impactos de ataques cibernéticos vão além dos danos técnicos. Fica evidenciado que os riscos repercutem em toda a estrutura organizacional. Essa interconexão reforça a necessidade de uma abordagem integrada de gestão de riscos, que considere não apenas a prevenção, mas também a preparação para responder a incidentes e mitigar seus efeitos.

Diante disso, torna-se fundamental a adoção de medidas de controle eficazes. Para isso, utilizou-se como referência o framework CIS Controls versão 8 (CIS v8), na Tabela 5 será evidenciado o controle e a explicação do mesmo associado aos riscos apresentados na Tabela 1.

Tabela 5. Aplicação dos Controles CIS na Mitigação de Riscos de Negócio

Risco de Negócio	Controle CIS	Definição e propósito do controle	Como o controle mitiga o risco
[1] Vazamento de dados pessoais de usuários	Controle 3 Proteção de dados	Desenvolver processos e controles técnicos para identificar, organizar, proteger, guardar e descartar dados de forma segura.	Implementa um ciclo de vida completo para os dados, que vai desde a classificação por nível de sensibilidade até a criptografia e o descarte seguro, garantindo a proteção das informações pessoais contra acessos indevidos e vazamentos.
[2] Indisponibilidade de sistemas de bilhetagem	Controle 11 Recuperação de Dados	Adotar e manter práticas eficazes de recuperação de dados que permitam restaurar os ativos a um estado seguro e funcional anterior ao incidente	Garante que, em situações de falha ou ataque (como ransomware), haja backups atualizados e testados, permitindo a rápida restauração dos sistemas de bilhetagem e reduzindo ao mínimo o tempo de indisponibilidade.
[3] Interrupção de serviços digitais	Controle 16 Segurança de Aplicativos	Controlar todas as etapas do ciclo de vida do software (seja ele desenvolvido internamente, hospedado ou	Garante que aplicativos e sites sejam criados e mantidos com boas práticas de segurança, corrigindo falhas que possam ser exploradas por atacantes

		adquirido) para evitar, identificar e corrigir falhas de segurança.	para provocar interrupções ou danos.
[4] Vazamento de documentos internos e dados sensíveis	Controle 3 Proteção de dados	Desenvolver processos e controles técnicos para identificar, organizar, proteger, guardar e descartar dados de forma segura.	Assim como na proteção de dados de usuários, este controle classifica e protege informações internas sensíveis por meio de criptografia e controle de acesso, prevenindo que sejam acessadas ou divulgadas indevidamente.
[5] Descumprimento de normas legais e regulatórias	Controle 3 Proteção de dados	Desenvolver processos e controles técnicos para identificar, organizar, proteger, guardar e descartar dados de forma segura.	Contribui para o cumprimento de normas, pois ao definir processos claros para o tratamento de dados pessoais, abrangendo a gestão de consentimento, o mapeamento dos dados e a garantia dos direitos dos titulares.
[6] Manipulação de informações operacionais	Controle 5 Configuração Segura de Ativos Corporativos e Software	Utilizar processos e ferramentas para definir e controlar as permissões de acesso de contas de usuário, incluindo contas de administradores e de serviços.	Garante que somente pessoas autorizadas tenham acesso e possam modificar informações operacionais. Ao controlar rigorosamente os privilégios de administrador, diminui-se o risco de alterações indevidas por usuários internos ou contas comprometidas.
[7] Perda de informações administrativas críticas	Controle 11 Recuperação de Dados	Adotar e manter práticas eficazes de recuperação de dados que permitam restaurar os ativos a um estado seguro e funcional anterior ao incidente.	Garante que dados administrativos essenciais façam parte de backups regulares e estejam devidamente protegidos, possibilitando a recuperação total em caso de perda acidental, falha de hardware ou ataque cibernético.

Fonte: Elaborado pelos autores (2025)

A Tabela 5 evidencia sobre a capacidade dos controles diante dos riscos de negócio, é notável como a aplicação de um único controle, como o CIS Control 03, é capaz de mitigar três dos sete riscos apresentados. Essa abordagem otimiza os recursos da organização, em virtude do alto valor para implementação da gestão de risco nas organizações. Para as companhias metroferroviárias, que lidam diariamente com um volume massivo de informações sensíveis, implementar esses controles essenciais não é apenas uma medida técnica, mas um pilar fundamental para garantir a confiança pública e a segurança de milhões de pessoas.

5. CONCLUSÃO E CONTRIBUIÇÕES

Considerando a crescente incidência de ataques cibernéticos em infraestruturas críticas, este estudo buscou identificar os riscos de negócio associados às atividades principais de companhias metroferroviárias, com o objetivo de analisar as possíveis relações com a necessidade de implementação de controles de segurança cibernética. O objetivo proposto foi atendido, uma vez que o trabalho conseguiu identificar os principais riscos de negócio a elas inerentes, estabelecer a vinculação entre fontes/causas e consequências e propor um controle como medida preventiva para os riscos.

Para a realização deste estudo, foi conduzida uma revisão bibliográfica sobre gestão de riscos e segurança cibernética em transportes, e utilizou-se o método *Bow Tie* para a análise dos dados coletados, bem como o framework CIS Controls v8 para a proposição de controles. A análise preliminar de perigos foi baseada em reportagens de casos reais de ataques cibernéticos a companhias metroviárias.

Diante da metodologia adotada, observa-se que uma limitação deste estudo foi a ausência de entrevistas com gestores e especialistas atuantes no setor metroferroviário. Embora a pesquisa bibliográfica e a análise de casos reais tenham fornecido uma base sólida para a identificação dos riscos, a inclusão de entrevistas poderia ter ampliado a profundidade da identificação dos riscos inerentes a esta esfera de atuação, enriquecendo a perspectiva prática e validando os resultados com base na experiência de campo.

Como trabalhos futuros, sugere-se ampliar o escopo da pesquisa para incluir a realização de entrevistas com profissionais e órgãos do setor metroferroviário, a fim de aprofundar a identificação e validação dos riscos de negócio. Propõe-se ainda que os riscos identificados sejam avaliados para fins de análise de criticidade, a continuidade da análise dos riscos operacionais relacionados ao negócio e a priorização dos controles de segurança cibernética necessários para o tratamento dos riscos de negócio mais relevantes, considerando as particularidades operacionais e regulatórias do transporte metropolitano.

AGRADECIMENTOS

Agradecemos à FAPDF pelo apoio por meio do Edital 06/2024 – FAP Learning.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO 31000: Gestão de riscos - Diretrizes.** 2. ed. Rio de Janeiro: ABNT, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 31010: Gestão de riscos - Técnicas para o processo de avaliação de riscos.** Rio de Janeiro: ABNT, 2012.

BARRAGAN, L. G.; WEFFORT, E. F. J.; ARANHA, M. P. S. **O processo de gestão de riscos e controles internos nas entidades sem fins lucrativos como uma ferramenta para redução de custos.** In: CONGRESSO BRASILEIRO DE CUSTOS, 13., 2006, Belo Horizonte. Anais [...]. São Leopoldo: Associação Brasileira de Custos, 2006.

BERGAMINI JUNIOR, S. **Controles internos como um instrumento de governança corporativa.** Revista do BNDES, v. 12, n. 24, p. 149-188, 2005.

BERMEJO, P. H. S. et al. **ForRisco: gerenciamento de riscos em instituições públicas na prática.** Brasília: Editora Evobiz, 2018.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Portaria nº 93, de 18 de outubro de 2021.** Aprova o glossário de segurança da informação. Diário Oficial da União: seção 1, Brasília, DF, n. 201, p. 8, 25 out. 2021.

BRASIL. Presidência da República. Secretaria-Geral. **Decreto nº 10.569, de 9 de dezembro de 2020.** Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Diário Oficial da União: seção 1, Brasília, DF, n. 236, p. 4, 10 dez. 2020.

CARVALHO, P. S. M. de. **A defesa cibernética e as infraestruturas críticas nacionais.** Coleção Meira Mattos - Revista das Ciências Militares, Rio de Janeiro, v. 7, n. 21, p. 27-40, 2011.

CENTER FOR CHEMICAL PROCESS SAFETY (CCPS). **Bow Ties in Risk Management: A Concept Book for Process Safety.** Hoboken: Wiley, 2018.

CORRÊA, R. L. **Interações Espaciais.** In: CASTRO, I. E.; GOMES, P. C. C.; CORRÊA, R. L. (org.). Explorações Geográficas: percursos no fim do século. Rio de Janeiro: Bertrand Brasil, 1997. p. 279-318.

DA SILVA, Edvan Gomes et al. **International perspectives on critical infrastructure: Evaluation criteria and definitions.** International Journal of Critical Infrastructure Protection, v. 48, art. 100761, 2025.

DZAZALI, S.; HUSSEIN ZOLAIT, A. **Assessment of information security maturity: an exploration study of Malaysian public service organizations.** Journal of Systems and Information Technology, v. 14, n. 1, p. 23-57, 2021.

ENCYCLOPAEDIA BRITANNICA. **Subway: underground railway system.** Disponível em: https://www.britannica.com/technology/subway. Acesso em: 26 jun. 2025.

ESTADÃO. **Ataque hacker ao Bilhete Único expõe dados de 13 milhões de pessoas.** Expresso, 23 dez. 2022. Disponível em: https://bit.ly/3JUZ3bU. Acesso em: 28 jul. 2025.

FERNANDES, F. C.; BEVETTI, J. E. **Gestão de risco em micro e pequenas empresas: uma pesquisa na região sul do Brasil.** In: ENCONTRO DE ESTUDOS SOBRE EMPREENDEDORISMO E GESTÃO DE PEQUENAS EMPRESAS (EGEPE), 8., 2014, Goiânia. Anais [...]. Curitiba: ANPAD, 2014.

FERNANDES, L. A.; GOMES, J. M. M. **Relatórios de pesquisa nas ciências sociais: características e modalidades de investigação.** ConTexto, Porto Alegre, v. 3, n. 4, p. 1-13, 2009. Disponível em:

https://seer.ufrgs.br/index.php/ConTexto/article/view/11638. Acesso em: 28 jul. 2025.

FERREIRA, A. C. dos S. **A vulnerabilidade em infraestruturas críticas.** 2020. Dissertação (Mestrado em Ciências Militares) – Instituto Universitário Militar, Lisboa, 2020.

FREITAS, R. V. **Equilíbrios econômico-financeiros das concessões.** São Paulo: Fórum, 2023.

G1. **Metrô de São Francisco libera catracas após ataque por vírus de resgate.** Segurança Digital, 28 nov. 2016. Disponível em: https://bit.ly/4nliXex Acesso em: 28 jul. 2025.

GAT. **Implementação do CIS Controls V8.** GAT Blog, 20 maio 2022. Disponível em: https://docs.gatinfosec.com/blog/implementacao-do-checklist-framework-cis-controls-v8/. Acesso em: 28 jul. 2025.

GOVERNO FEDERAL. **Segurança de infraestruturas críticas.** [2022]. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-de-infraestruturas-criticas. Acesso em: 28 jul. 2025.

INSTITUTO PORTUGUÊS DA QUALIDADE (IPQ). **NP ISO 31000:2018: Gestão do risco: linhas de orientação.** Lisboa: IPQ, 2018.

JUNIOR, G. do L. S. et al. **Gestão de risco no setor público.** Revista de Gestão e Secretariado, v. 14, n. 6, p. 9232-9245, 2023.

KOUR, R.; KARIM, R.; THADURI, A. **Segurança cibernética para ferrovias – Um modelo de maturidade.** Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, v. 234, n. 10, p. 1129-1148, 2020.

LAKATOS, E. M.; MARCONI, M. A. **Técnicas de pesquisa.** 4. ed. São Paulo: Atlas, 1985.

LIMA, E. d. et al. **Avaliação da rotina operacional do operador nacional do sistema elétrico brasileiro (ONS) em relação às ações de gerenciamento de riscos associados à segurança cibernética.** RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, n. 49, p. 301-312, 2022.

LIN, D. et al. **Metro systems: construction, operation, and impacts.** Tunnelling and Underground Space Technology, v. 143, art. 105373, 2024. DOI: https://doi.org/10.1016/j.tust.2023.105373.

MACHADO, M. R.; BAX, M. P. **Utilização de ontologia para auxílio na avaliação de segurança cibernética da infraestrutura crítica do setor elétrico: perspectiva brasileira.** In: SEMINAR ON ONTOLOGY RESEARCH IN BRAZIL; DOCTORAL AND MASTERS CONSORTIUM ON ONTOLOGIES, 13., 2020, Vitória. Anais [...]. Belo Horizonte: Universidade Federal de Minas Gerais, 2020.

MALATJI, M.; MARNEWICK, A. L.; VON SOLMS, S. **Capacidades de segurança cibernética para resiliência de infraestrutura crítica.** Information & Computer Security, v. 30, n. 2, p. 255-279, 2022.

METRÔ CPTM. **Grupo hacker assume autoria por invasão dos servidores da CPTM.** 29 dez. 2022. Disponível em: https://bit.ly/3VE7s62. Acesso em: 28 jul. 2025.

MICROSOFT. **Parâmetros da Center For Internet Security (CIS).** Redmond: Microsoft, 21 set. 2023. Disponível em: https://www.microsoft.com. Acesso em: 28 jul. 2025.

MONITOR DO ORIENTE. **Ataque cibernético atinge ministério e ferrovia do Irã.** 11 jul. 2021. Disponível em: https://bit.ly/4m58Mty. Acesso em: 28 jul. 2025.

MOREIRA, Fernando Rocha; DA SILVA FILHO, Demétrio Antônio; AMVAME NZE, Georges Daniel; DE SOUSA JÚNIOR, Rafael Timóteo; NUNES, Rafael Rabelo. **Evaluating the performance of NIST's Framework Cybersecurity Controls through a constructivist multicriteria methodology.** IEEE Access, v. 9, p. 129605-129618, 2021. DOI: https://doi.org/10.1109/ACCESS.2021.3113178.

MOURA, J. X. **Processo de adoção do sistema de informação SIPAR-Diligência no Ministério da Saúde.** 2. ed. 3. reimp. Brasília, DF: Ministério da Saúde, 2016. (Série A. Normas e Manuais Técnicos).

NBC WASHINGTON. **A cyberattack took down Metro's website for two hours. Here's what a cybersecurity expert says.** NBC Washington, 7 maio 2024. Disponível em: https://bit.ly/3VEfhIX. Acesso em: 28 jul. 2025.

PARDO, J. A. R. **Metodologia para análise e gestão de riscos em pavimentos ferroviários.** 2009. 187 f. Dissertação (Mestrado em Geotecnia) – Universidade Federal de Ouro Preto, Ouro Preto, 2009.

RELIM, Tiago Eny; OLIVEIRA, Edgard Costa; MARIANO, Ari Melo; GRUBISIC, Viviane Vasconcellos Ferreira. **Capital econômico para risco de crédito: gestão de riscos do processo de cálculo por meio da aplicação da norma ABNT ISO 31000 e da matriz G.U.T.** Brazilian Journal of Development, v. 6, n. 5, p. 25369-25384, 2020. DOI: https://doi.org/10.34117/bjdv6n5-115.

SILVA, E. **Cibersegurança das infraestruturas críticas nacionais.** 2015. Monografia (Curso de Especialização em Segurança da Informação e Comunicações) – Universidade de Brasília, Brasília, DF, 2015.

SILVA, E. L.; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação.** Florianópolis: Editora da UFSC, 2005.

TECMUNDO. **Metrô da Dinamarca pode rodar após sofrer ataque hacker massivo.** TecMundo, 14 maio 2018. Disponível em: https://bit.ly/46e9TRR. Acesso em: 28 jul. 2025.

TECMUNDO. **Ucrânia sofre ciberataque em infraestrutura de aeroporto e metrô.** TecMundo, 24 out. 2017. Disponível em: http://bit.ly/4m3RmxD. Acesso em: 28 jul. 2025.

TONN, Gina; KESAN, Jay P.; ZHANG, Linfeng; CZAJKOWSKI, Jeffrey. **Cyber risk and insurance for transportation infrastructure.** Transport Policy, v. 79, p. 103-114, 2019. DOI: https://doi.org/10.1016/j.tranpol.2019.04.019.