Rede Federal em alerta: riscos de negócio para segurança cibernética na Educação Profissional, Científica e Tecnológica

Lídia Bononi P. Tomaz[1], **Rafael Rabelo Nunes**[2], **Ígor Ramos Bezerra da Silva**[2]

[1]Instituto Federal do Triângulo Mineiro (IFTM)
Campus Uberaba Parque Tecnológico
Uberaba - MG

[2]Departamento de Engenharia Elétrica
Universidade de Brasília
Brasília - DF

lidia@iftm.edu.br,{igorramos1, rafaelrabelo}@unb.br

Abstract. *The advancement of digital transformation in institutions of the Federal Network of Professional, Scientific and Technological Education (RFEPCT) has expanded access to digital services but has also increased their exposure to cyber risks. This scenario is further aggravated by the growing incidence of information security incidents in recent years. Despite the existence of guidelines, such as the controls established in the Federal Government's Privacy and Information Security Program (PPSI), many RFEPCT institutions face difficulties in recognizing their main weaknesses and vulnerabilities. In this context, this study proposes a practical methodology for identifying key business risks related to information security that directly impact the core activities of teaching, research, and extension within the RFEPCT. The methodology was applied to the Instituto Federal do Triângulo Mineiro (IFTM) as a case study, through questionnaires administered to staff members and the use of the Bow Tie technique to map events, causes, and consequences. The results revealed seven business risks, linked to 36 causes and 21 consequences, highlighting risk management as an essential tool for governance and cyber resilience.*

Resumo. *O avanço da transformação digital nas instituições da Rede Federal de Educação Profissional, Científica e Tecnológica (RFEPCT) ampliou o acesso a serviços digitais, mas também elevou sua exposição a riscos cibernéticos. Esse cenário é agravado pela crescente incidência de incidentes de segurança da informação na atualidade. Apesar da existência de diretrizes, como os controles definidos no Programa de Privacidade e Segurança da Informação (PPSI) do Governo Federal, muitas instituições da RFEPCT enfrentam dificuldades em reconhecer suas principais fragilidades e vulnerabilidades. Nesse contexto, este trabalho propõe uma metodologia prática para identificar os principais riscos de negócio relacionados à segurança da informação que afetam diretamente as atividades finalísticas de ensino, pesquisa e extensão da RFEPCT. Adotou-se como estudo de caso o Instituto Federal do Triângulo Mineiro (IFTM), por meio da aplicação de questionários a servidores e da utilização da técnica Bow Tie para mapear eventos, causas e consequências. Os resultados revelaram sete riscos de negócio, vinculados a 36 causas e 21 consequências, evidenciando a*

gestão de riscos como ferramenta essencial para governança e resiliência cibernética.

1. Introdução

Nos últimos anos, o avanço da transformação digital no setor público brasileiro — especialmente após a promulgação da *Estratégia de Governo Digital*, atualmente vigente até 2027 [Brasil 2024] — impulsionou as instituições de ensino da Rede Federal de Educação Profissional, Científica e Tecnológica (RFEPCT) [Brasil 2008] a digitalizarem progressivamente seus processos administrativos e acadêmicos. A pandemia de COVID-19 acelerou ainda mais esse processo, exigindo a digitalização de atividades como matrículas, solicitações acadêmicas e emissão de documentos. Embora essa modernização tenha ampliado o acesso e a eficiência dos serviços prestados, ela também aumentou de forma significativa a exposição dessas instituições a riscos cibernéticos.

De fato, o número de incidentes cibernéticos tem crescido continuamente. Segundo o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (CTIR Gov), considera-se incidente "qualquer evento adverso, confirmado ou sob suspeita, que comprometa a segurança de sistemas e redes computacionais" [CTIR-Gov 2025a]. Em 2024, o CTIR Gov registrou um aumento de 48% nas notificações de incidentes em relação ao ano anterior [CTIR-Gov 2025b]. Especificamente no setor educacional, dados da [CrowdStrike 2025] indicam que instituições acadêmicas figuram entre os principais alvos de ataques cibernéticos em escala global. Esse cenário se explica pelo grande volume de dados sensíveis e pessoais de estudantes, além de informações relacionadas à propriedade intelectual que essas instituições armazenam. Soma-se a isso o fato de que, por vezes, estudantes buscam explorar vulnerabilidades nos sistemas como forma de testar seus conhecimentos. No Brasil, casos noticiados pela imprensa envolvendo ataques a Instituições Federais de Ensino, como [G1 Paraná 2021, G1 Mato Grosso do Sul 2023, G1 Piauí 2024, G1 Amapá 2024], reforçam essa realidade.

Para apoiar as organizações a lidar com esse cenário, diversos frameworks internacionais, como o *Cybersecurity Framework* do NIST [NIST 2024] e os *CIS Controls* [CIS 2025], oferecem diretrizes para fortalecer a resiliência cibernética. No contexto brasileiro, o Governo Federal lançou o Programa de Privacidade e Segurança da Informação (PPSI), com o objetivo de elevar o nível de maturidade de instituições como as que fazem parte da RFEPCT, por comporem o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) [MGI 2023].

Entretanto, a implementação efetiva dessas medidas na RFEPCT enfrenta desafios concretos. Destacam-se, entre eles, a dificuldade da alta administração em reconhecer as fragilidades existentes nas próprias instituições, bem como a necessidade de que os profissionais de segurança da informação compreendam com clareza quais ativos e processos são prioritários para proteção. Nesse contexto, a adoção de práticas sistemáticas de gestão de riscos em segurança da informação deixa de ser uma ação pontual e torna-se uma exigência fundamental. Essa abordagem é essencial tanto para assegurar a conformidade com as exigências legais quanto para elevar o nível de maturidade institucional, garantindo os princípios fundamentais da segurança da informação — confidencialidade, integridade e disponibilidade — em um cenário marcado pela crescente digitalização dos serviços públicos educacionais.

Apesar da relevância do tema, um levantamento realizado com dirigentes das áreas de Tecnologia da Informação de 41 instituições da RFEPCT — compostas pelos Institutos Federais, CEFETs e o Colégio Pedro II — revelou que apenas 15% dessas organizações possuem processos estruturados de gestão de riscos voltados à área de Tecnologia da Informação [FORTI 2025]. Diante desse cenário, o presente trabalho propõe uma metodologia prática para identificação de riscos de negócio relacionados à segurança da informação, com foco nas atividades finalísticas da RFEPCT. A abordagem foi aplicada ao Instituto Federal do Triângulo Mineiro (IFTM) devido ao vínculo dos autores com a instituição e ao fato de que as instituições da RFEPCT compartilham uma base legal comum.

Os resultados revelaram sete riscos de negócio associados a um conjunto diversificado de causas e consequências. Embora tais riscos de negócio não possam ser generalizados para toda a RFEPCT, considerando que muitos dos desafios enfrentados pelo IFTM são representativos da realidade de outras instituições desta Rede, este levantamento oferece *insights* estratégicos que podem apoiar os gestores institucionais na compreensão dos riscos de negócio que permeiam suas atividades finalísticas. O mapeamento realizado visa fornecer subsídios qualificados para a formulação de medidas estratégicas de mitigação, fortalecendo a governança em segurança da informação, assegurando a continuidade dos serviços educacionais e impulsionando a maturidade institucional na gestão de riscos no setor público educacional. Espera-se, assim, que os achados desta pesquisa se configurem como uma ferramenta útil à alta administração, favorecendo uma atuação proativa, orientada à identificação de fragilidades e à adoção de condutas preventivas diante das ameaças que possam comprometer a missão institucional.

Este trabalho está estruturado da seguinte forma: a Seção 2 apresenta os principais conceitos teóricos que fundamentam a pesquisa; a Seção 3 descreve a metodologia empregada; a Seção 4 apresenta e analisa os resultados obtidos; e, por fim, a Seção 5 traz as conclusões do estudo e propõe direções para trabalhos futuros.

2. Referencial Teórico

Nessa seção apresentam-se os conceitos necessários para que se compreenda esse trabalho. Primeiramente, discorre-se sobre Riscos e Gestão de Riscos na Seção 2.1. Na sequência, a Seção 2.2 apresenta a visão geral da RFEPCT e as características particulares dos Institutos Federais. Além disso, a Seção 2.3 apresenta alguns trabalhos correlatos a esta pesquisa.

2.1. Risco e Gestão de Riscos

O risco é definido como o "efeito da incerteza nos objetivos" organizacionais [ABNT 2023]. Esse efeito corresponde a desvios em relação ao que se espera atingir, podendo ser positivos ou negativos. Ao passo que a incerteza se caracteriza pela ausência ou insuficiência de informações relacionadas à compreensão de eventos, suas causas, consequências ou probabilidades de ocorrência.

De fato, não existe risco zero. Ele é inerente a qualquer atividade humana ou institucional e, embora seja impossível eliminá-lo completamente, ele pode - e deve - ser gerenciado de forma sistemática e contínua [ABNT 2023]. Ademais, os riscos podem ser vistos como ameaças ou oportunidades. Neste último caso, convém destacar que avanços

e inovações ocorrem justamente porque indivíduos e instituições se dispõem a assumir riscos calculados — o que impulsiona o progresso e a competitividade [Alves et al. 2023]. No contexto de ameaça, merecem atenção, pois podem causar prejuízos à organização.

Como observam [Crouhy et al. 2014], cabe à organização não apenas reconhecer seus riscos, mas tomar decisões quanto à melhor forma de lidar com eles: mitigando, aceitando, transferindo ou evitando. Para isso, torna-se necessário identificar os riscos, medir a exposição a eles, analisar seus efeitos, avaliar os controles existentes e definir estratégias adequadas de mitigação, seguidas de avaliações críticas e revisões sistemáticas do desempenho do processo de gestão. Esse conjunto de atividades é denominado gestão de riscos.

A gestão de riscos pode ser compreendida como um conjunto de atividades coordenadas para dirigir e controlar uma organização em relação aos riscos que enfrenta. Segundo a [ABNT 2018], a gestão de riscos contribui para a criação e a proteção de valor, auxiliando organizações a estabelecerem estratégias, tomarem decisões mais bem-informadas e atingirem seus objetivos de forma mais eficaz.

No campo da segurança da informação, os riscos assumem especial importância diante da crescente digitalização e dependência tecnológica das organizações. Como discutem [Alves et al. 2023], a identificação e o tratamento dos riscos relacionados à segurança da informação são essenciais para a proteção da confidencialidade, integridade e disponibilidade dos dados. A falha em gerenciar esses riscos pode comprometer não apenas a continuidade das operações, mas também a conformidade com legislações como a Lei Geral de Proteção de Dados (LGPD) [Brasil 2018].

Nesse aspecto, convém salientar que todo o processo de transformação digital aumenta a superfície de exposição ao risco das organizações. Neste aspecto, a gestão de riscos é uma ferramenta fundamental para apoiar as organizações a manter seus valores para a sociedade. Assim, uma gestão de riscos eficaz deve ser integrada à governança institucional e à cultura organizacional, promovendo a resiliência institucional, a melhoria contínua e a geração de valor público.

2.2. A Configuração da RFEPCT

A Rede Federal de Educação Profissional, Científica e Tecnológica (RFEPCT), instituída pela Lei nº 11.892/2008 [Brasil 2008], é composta por Institutos Federais (IFs), CEFETs, UTFPR, Escolas Técnicas vinculadas a Universidades Federais e o Colégio Pedro II. Enquanto a UTFPR e as Escolas Técnicas mantêm vínculos administrativos com as Universidades, os 38 IFs, 2 CEFETs e o Colégio Pedro II são representados pelo CONIF (Conselho Nacional das Instituições de Educação Profissional, Científica e Tecnológica), que atua na formulação de políticas e no fortalecimento institucional [CONIF 2025]. Criados a partir dessa legislação, os IFs introduziram um modelo inovador, com estrutura multicurricular e atuação integrada na educação básica, superior e de jovens e adultos, promovendo a articulação entre ensino, pesquisa e extensão como processos finalísticos, conforme a Cadeia de Valor Integrada da Educação [MGI 2025, IFTM 2025].

Os IFs possuem estrutura própria e autonomia administrativa, financeira, patrimonial, didático-pedagógica e disciplinar, conforme o artigo 207 da Constituição Federal. Cada IF é composto por uma reitoria e diversos campi distribuídos regionalmente, permitindo atuação descentralizada e alinhada às demandas locais. Diferentemente das

Universidades Federais, os IFs seguem um modelo organizacional mais padronizado, regulamentado por portarias do MEC, como a Portaria nº 713/2021 [Brasil 2021], que estabelece critérios para o dimensionamento dos campi e a alocação de pessoal conforme o porte e complexidade institucional. Além disso, os IFs adotam um modelo exclusivo de distribuição orçamentária, baseado em indicadores da Plataforma Nilo Peçanha (PNP) [Ministério da Educação 2025], como o número e a situação das matrículas e a Relação Matrícula por Professor (RAP), fundamentais para a definição do orçamento institucional [de Oliveira et al. 2022].

Diante de sua estrutura regulamentada e da dependência de critérios técnicos para alocação de recursos, os Institutos Federais estão expostos a riscos que podem comprometer sua organização, infraestrutura e orçamento. Nesse cenário, a adoção sistemática da gestão de riscos torna-se fundamental para mitigar ameaças, aproveitar oportunidades e reforçar o papel estratégico dos IFs na consolidação da política pública de educação profissional no Brasil.

2.3. Trabalhos Correlatos

A literatura apresenta contribuições voltadas à gestão de riscos em segurança da informação no contexto de instituições públicas de ensino. Esses estudos evidenciam a crescente preocupação com a adoção de práticas sistematizadas e alinhadas a frameworks reconhecidos internacionalmente, como forma de mitigar vulnerabilidades e fortalecer a governança institucional.

Tanto [Silva 2017] quanto [Batista 2022] evidenciam a carência de políticas estruturadas de gestão de riscos da segurança da informação nas Instituições Federais de Ensino Superior (IFES), revelando um baixo grau de maturidade institucional nesse campo. O trabalho de [Silva 2017] propõe um conjunto de diretrizes estratégicas fundamentadas em normas internacionais, destacando a importância do apoio da alta administração, da definição clara de papéis e responsabilidades, do comprometimento da direção, do mapeamento sistemático dos riscos e da conscientização dos *stakeholders*. Em consonância, [Batista 2022] apresenta um modelo integrado e simplificado de ações identificando lacunas críticas na estrutura e na cultura de segurança da informação. Ambas as pesquisas convergem ao apontar a necessidade de apoio institucional efetivo, alocação de recursos financeiros e fortalecimento da cultura organizacional para a implementação consistente da gestão de riscos nas IFES.

No Instituto Federal de São Paulo (IFSP), [Souza et al. 2020] analisaram o tratamento da segurança da informação por meio de um estudo empírico com gestores da área de tecnologia da informação. Os autores constataram práticas ainda embrionárias e a ausência de alinhamento efetivo com padrões como da ABNT ISO/IEC 27001:2022 [ABNT 2022]. O estudo enfatizou que a governança de TI, quando integrada à gestão de riscos, pode oferecer bases mais sólidas para a tomada de decisões e a mitigação de ameaças operacionais.

Não se identificou estudos que objetivassem identificar de forma objetiva quais seriam os riscos de negócio de instituições federais de educação, em especial da RFEPCT.

3. Metodololgia

Este trabalho caracteriza-se como uma pesquisa de natureza aplicada, com abordagem qualitativa, caráter exploratório e procedimento metodológico de levantamento. A pesquisa é classificada como aplicada por buscar a geração de conhecimento voltado à resolução de problemas concretos e imediatos. Sua abordagem qualitativa permite explorar dimensões da realidade que não se prestam à quantificação, com ênfase na compreensão aprofundada das dinâmicas organizacionais e sociais [Lozada and Nunes 2018]. O caráter exploratório se justifica pelo propósito de fornecer uma visão inicial sobre os riscos de negócio em instituições da RFEPCT, conforme Gil (2012, p. 27 *apud* [Lozada and Nunes 2018]), que aponta esse tipo de pesquisa como útil na formulação de hipóteses e na delimitação de problemas. O levantamento foi adotado como procedimento metodológico em razão da coleta de dados junto a um grupo definido de participantes [Wazlawick 2021].

As etapas desenvolvidas ao longo da pesquisa estão ilustradas na Figura 1.

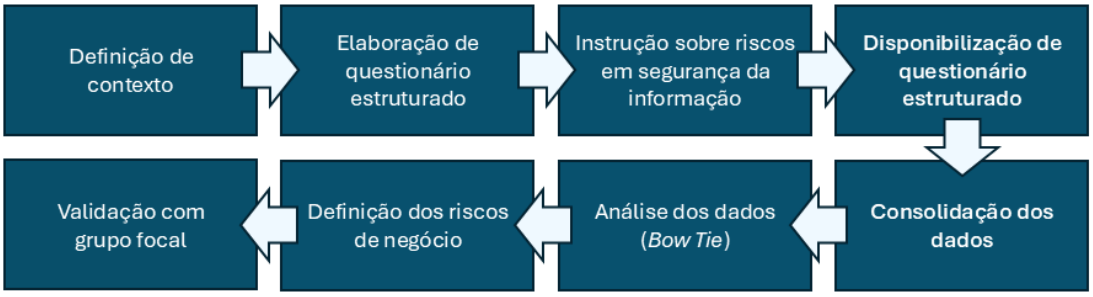

Figura 1. Etapas da pesquisa

A definição de contexto focou as áreas finalísticas do IFTM — ensino, pesquisa e extensão — com base na Cadeia de Valor Integrada da Educação (Seção 2). Essas atividades, por sua natureza, envolvem o tratamento sistemático de dados pessoais de estudantes, servidores e colaboradores, o que acentua a necessidade de gestão adequada dos riscos relacionados à segurança da informação e à privacidade.

Na etapa seguinte, elaborou-se um questionário estruturado com o objetivo de captar a percepção dos servidores sobre eventos que pudessem comprometer a confidencialidade, a integridade e a disponibilidade das informações. O instrumento incluiu campos para descrição dos eventos, causas percebidas, consequências possíveis, frequência observada, impacto institucional e sugestões de mitigação. Não foram coletados dados pessoais ou de e-mail, garantindo o anonimato dos respondentes. O questionário foi disponibilizado via Google Forms, selecionado pela acessibilidade e pela capacidade de atingir servidores em diferentes campi. O modelo está disponível em: *https://bit.ly/4dQWVg6*.

A escolha do questionário estruturado como principal instrumento de coleta de dados foi estratégica e fundamentada nas particularidades do IFTM. Diferentemente de outras metodologias como entrevistas e grupos focais, que, embora ricas, seriam mais restritivas, o questionário permitiu levar a proposta do trabalho a um público amplo e diversificado, dada a distribuição dos servidores por diferentes campi. Essa abordagem se mostrou ideal, visto que as instituições da RFEPCT, incluindo o IFTM, compartilham

uma base legal e estruturas organizacionais similares, tornando a percepção dos servidores de diferentes unidades relevante para o estudo de caso.

Para promover o alinhamento conceitual entre os participantes, realizaram-se sessões instrutivas sobre riscos em segurança da informação, com duração média de 30 minutos. Os conteúdos foram baseados nas diretrizes das normas ABNT NBR ISO/IEC 27005:2023 [ABNT 2023] e ABNT NBR ISO/IEC 31000:2018 [ABNT 2018], abordando os conceitos de risco, ameaça e vulnerabilidade. Além do embasamento teórico, buscou-se enfatizar o papel ativo dos servidores na identificação de riscos institucionais, valorizando o conhecimento prático oriundo das suas rotinas de trabalho. A participação foi voluntária e aberta a todos os servidores das áreas finalísticas, independentemente do exercício de cargos comissionados ou funções gratificadas. Destaca-se que o engajamento dos gestores de cada unidade foi crucial para o êxito da ação. Além disso, é importante ressaltar que esses momentos foram fundamentais para motivar a participação na pesquisa.

O questionário permaneceu disponível por um período definido em conjunto com os participantes. Após a coleta, os dados foram consolidados, segmentados e padronizados para análise. Respostas com múltiplos eventos foram desmembradas, duplicidades foram removidas, e causas ou efeitos implícitos foram explicitados com base na análise contextual. A técnica *Bow Tie* foi utilizada para representar graficamente os riscos, destacando suas causas e consequências. Esta técnica é indicada para representar riscos que possuem uma gama de causas possíveis e consequências, conforme expõe a ABNT NBR ISO/IEC 31010:2012 [ABNT 2012]. Ainda que a técnica *Bow Tie* permita a representação de controles preventivos e mitigatórios, esta ação não está contemplada escopo desta pesquisa.

É importante ressaltar que a estratégia de se utilizar o instrumento do questionário aliado à atividade de instrução sobre riscos em segurança da informação foi adotada visando atingir a diversidade de público do IFTM que estão alocados em diversos campi, que possuem estruturas semelhantes em relação às áreas finalísticas. Além disso, visou dar um embasamento inicial e acolhimento dos participantes motivando-os a contribuir com suas experiências. Logo, o questionário trouxe maior liberdade para os participantes, visto que eles puderam refletir em suas atividades e puderam expor sem constrangimento dado o caráter de anonimato adotado. O instrumento do questionário também permitiu divulgar o trabalho a mais servidores, visto que outras metodologias como entrevistas seriam mais demoradas para realizar a coleta e consolidação dos dados. A análise de grupo focal também seria impactada, pois a pluralidade dos campi poderia ser comprometida pela restrição de participantes do grupo. Assim, a escolha do instrumento se mostrou adequada à ampla participação dos servidores da instituição.

A análise resultou na identificação de um conjunto de riscos de negócio relevantes para o IFTM, com potencial de aplicação a outras instituições da RFEPCT. Esses riscos foram validados por meio de grupo focal, composto por especialistas da instituição com atuação em gestão de riscos e segurança da informação. O objetivo dessa etapa foi verificar a aderência dos riscos à realidade institucional e promover eventuais ajustes ou refinamentos nas categorias identificadas.

ID	Riscos de Negócio
1	Vazamento de dados pessoais/sensíveis de estudantes, servidores ou terceirizados (CPF, endereço, dados bancários etc.)
2	Vazamento de dados de propriedade intelectual
3	Perda de informações (estudantes, docentes, ofertas de turmas, projetos, etc.)
4	Comprometimento da integridade dos dados de ensino, pesquisa ou extensão
5	Emissão de documentos institucionais incorretos (diplomas, históricos, certificados, etc.)
6	Impacto nos indicadores institucionais da Política Nacional de Permanência (PNP)
7	Não conformidade com exigências regulatórias e legais

Tabela 1. Riscos de negócio mapeados na PROEN/IFTM

4. Resultados

Este estudo buscou identificar os principais riscos de negócio das áreas finalísticas de ensino, pesquisa e extensão de instituições da RFEPCT usando como estudo de caso o IFTM. O levantamento dos eventos foi feito por meio da aplicação de um questionário estruturado, conforme apresentado na Seção 3. Houve 33 respostas de servidores de diferentes setores e responsabilidades na administração que expuseram situações/eventos do cotidiano.

Cada resposta do formulário foi direcionada a um evento/situação do setor. Todavia, notou-se que algumas respostas relatavam mais de uma situação. O questionário também apresentou aos participantes questões para coletar a sua visão em relação às possíveis causas e consequências, bem como a frequência das situações relatadas. Esses dados, apesar de não pertencerem à etapa de identificação dos riscos, permitiram que os participantes refletissem e fornecessem suas percepções sobre cada situação. Também foi deixado um espaço opcional para que os participantes pudessem expor meios de mitigar a situação/evento indicado. Esses campos foram usados para apoiar na etapa de análise dos riscos, visando estabelecer a relação das suas causas e consequências a partir do método *Bow Tie*.

Ao final das etapas desta pesquisa, foram obtidos os riscos de negócio relacionados na Tabela 1. Cada risco possui um conjunto de causas e consequências apresentadas nas Tabelas 2 e 3, respectivamente. No geral, este conjunto de riscos estão relacionados a 36 causas possíveis e 21 consequências. A relação completa entre estes riscos de negócio com suas respectivas causas e consequências pode ser acessada em *https://bit.ly/riscosrfepct*.

4.1. Discussão dos resultados

Ao analisar os riscos apresentados na Tabela 1, constata-se que certos eventos — como o vazamento de dados pessoais ou de propriedade intelectual, a emissão indevida de documentos institucionais, a perda de informações relativas a estudantes e servidores, a integridade de dados vinculados ao ensino, à pesquisa e à extensão, bem como a não conformidade regulatória — configuram-se como riscos inerentes às instituições de ensino e pesquisa científica, como aquelas pertencentes à RFEPCT e às Universidades Federais, conforme demonstra o trabalho de [Gonçalves et al. 2025]. Por outro lado, riscos relacionados ao impacto nos indicadores institucionais da PNP apresentam-se como específicos das instituições da RFEPCT, dada sua vinculação direta a normativos próprios que regulamentam sua estrutura organizacional e os critérios de avaliação e financiamento, conforme

Tabela 2. Causas e efeitos associados aos riscos mapeados

Causas e efeitos	Riscos associados
Acesso aos sistemas por terceiros com credenciais válidas	1, 2, 3, 4, 5, 6
Acesso não autorizado a servidor de arquivos	4, 5
Alteração de legislação com curto prazo para adequação	7
Alterações de dados por pessoa não autorizada	3, 5
Ataque cibernético ou engenharia social	1, 2, 3, 4, 5
Classificação inadequada dos documentos digitais	1, 2
Condutas inadequadas ou negligência de usuários	1, 2, 4
Deficiência na rastreabilidade dos dados e controle de alterações	1, 2
Desalinhamento entre as unidades da instituição	6
Desconhecimento ou dificuldade na compreensão da legislação	7
Descuido no uso do computador	1, 2
Erros humanos no lançamento de dados nos sistemas	5, 6
Excesso de privilégios no sistema	1, 2, 5
Falha tecnológica (código-fonte) nos softwares	1, 2, 3, 4, 5
Falta de backup e recuperação de dados	4
Falta de capacitação dos servidores sobre tratamento de dados e LGPD	1
Falta de checklist/processo para emissão de documentos	3
Falta de integração entre diferentes fontes de dados	3, 5, 6
Falta de procedimentos claros ou processos ineficientes	1, 2, 3, 5, 6
Falta de validação automatizada de dados	4, 5
Incapacidade de pessoal para atender aos novos programas governamentais	7
Inconsistência dos dados do sistema de software devido às regras de negócio mal definidas	5, 6
Indisponibilidade de infraestrutura tecnológica	4
Ineficiência na execução orçamentária	6
Movimentação de dados por meio de pendrive, cartões de memória e notebooks	1, 2, 4
Não anonimização de dados em documentos com grau de sigilo público	1
Normativos/processos desatualizados	7
Perda de matrículas	6
Procedimentos manuais	6
Rotatividade de servidores nos setores	3
Sobrecarga de trabalho	1, 3
Uso de computadores pessoais “desprotegidos”	1, 2, 4
Utilização de arquivos armazenados localmente em estações de trabalho	4
Utilização de ferramentas não oficiais para comunicação institucional	1, 2
Utilização de rede não segura no teletrabalho	1, 2, 4
Vazamento de senha (senha fraca, compartilhamento de senha, não troca de senhas nas mudanças setoriais)	1, 2, 5

Fonte: Elaboração própria.

explanado na Seção 2.2.

A Tabela 2 evidencia que uma mesma causa pode estar associada a múltiplos riscos. De forma análoga, observa-se na Tabela 3 que um único risco pode resultar em diversas consequências. Um aspecto adicional que merece destaque é o encadeamento entre causas e efeitos: determinadas consequências podem, por sua vez, configurar novas causas, evidenciando a complexidade e a interdependência entre os elementos analisados.

Outro ponto relevante é que diversas causas identificadas estão fortemente relacionadas a questões operacionais. Esse aspecto evidencia que, embora originados no

Tabela 3. Consequências associadas aos riscos mapeados

Consequências	Riscos associados
Acionamento por órgãos de controle	1, 2, 3, 7
Bloqueio no crescimento da instituição em relação a número de servidores	6
Dados inconsistentes nos sistemas SISTEC e PNP	5
Dano econômico por perda de licenças e registros	2
Emissão de documentos oficiais (histórico, diplomas, certificados) indevidamente (com dados falsos/adulterados)	5
Impacto na busca de recursos junto ao Governo Federal	6, 7
Impacto na continuidade dos serviços	4
Impactos nos registros dos indicadores acadêmicos	4, 6
Ineficiência na tomada de decisão	4, 6
Não conformidade com legislação vigente	6, 7
Perda da memória institucional	1, 2, 4
Perda de confiabilidade na gestão da instituição	1, 2, 3, 4, 5, 6
Perda de credibilidade dos sistemas institucionais	6
Perda de potencial inovador em projetos	2
Prejuízo à imagem institucional	1, 2, 3, 4, 5, 7
Prejuízo ao clima organizacional (retrabalho, desconfianças, sobrecarga de trabalho)	1, 2, 4, 5
Prejuízo no orçamento da instituição que é baseado nos dados da PNP	6
Problemas para realização de prestação de contas	4
Responsabilização do servidor	4, 5
Responsabilização legal da instituição	1, 2, 3, 4, 5, 6
Violação à LGPD	1

Fonte: Elaboração própria.

nível operacional, os riscos resultantes têm impacto significativo nos níveis tático e estratégico da instituição. Essa constatação reforça a necessidade do envolvimento da alta administração no reconhecimento e na compreensão dos riscos, de modo a subsidiar decisões mais informadas e alinhadas aos objetivos institucionais.

As respostas obtidas por meio do questionário também revelaram ações mitigatórias sugeridas pelos participantes, tais como a melhoria na comunicação institucional, o mapeamento de processos, a integração entre sistemas internos e governamentais, além da oferta contínua de capacitações. Embora este trabalho não tenha como escopo a proposição de controles específicos, tais sugestões indicam a percepção, por parte dos respondentes, de que existem possibilidades concretas de mitigação dos riscos enfrentados no cotidiano institucional.

Por fim, é crucial reconhecer a limitação de que esta pesquisa, por ter sido conduzida em uma única instituição da RFEPCT, tem resultados que não podem ser generalizados. Todavia, os riscos de negócio identificados funcionam como uma base sólida para que outras instituições da Rede iniciem suas próprias análises, enquanto a metodologia proposta serve como um guia para um mapeamento personalizado e contextualizado. Para que esse processo seja bem-sucedido, é indispensável o comprometimento da alta administração em cada instituição. No IFTM, o interesse manifestado por sua gestão em relação aos resultados desta pesquisa reforça o valor do estudo e demonstra uma postura proativa em reconhecer vulnerabilidades e adotar estratégias para fortalecer a resiliência organizacional.

5. Conclusões e Trabalhos Futuros

Este trabalho teve como objetivo identificar os principais riscos de negócio relacionados à segurança da informação que impactam diretamente as atividades finalísticas de ensino, pesquisa e extensão em instituições da RFEPCT, tendo como estudo de caso o IFTM. A partir da aplicação de um questionário estruturado e da utilização da técnica *Bow Tie*, foram mapeados sete riscos centrais, associados a 36 causas e 21 consequências distintas.

Os resultados revelaram que, embora muitas causas estejam ligadas a falhas operacionais, os impactos desses riscos se manifestam de forma significativa nos níveis tático e estratégico da gestão. Embora os achados não possam ser generalizados para todas as instituições da RFEPCT, os riscos de negócio identificados podem servir de diretriz para que outras organizações da Rede conduzam o mesmo procedimento. É importante notar que, embora se assemelhem aos riscos de negócio identificados em Universidades Federais, eles possuem particularidades quanto ao impacto nos indicadores institucionais da PNP.

Dessa forma, além de contribuir para o fortalecimento da maturidade em gestão de riscos no âmbito da RFEPCT, os achados desta pesquisa oferecem subsídios práticos para que a alta administração atue de forma preventiva e estratégica frente aos riscos cibernéticos. Como perspectivas para trabalhos futuros, propõe-se: (i) o aprofundamento da análise dos riscos identificados, com a proposição de controles mitigatórios específicos; (ii) a vinculação entre as causas mapeadas e os controles previstos no PPSI; e (iii) a construção de um framework para gestão de riscos de segurança da informação nas instituições da RFEPCT, visando à consolidação de um referencial nacional para a Rede Federal.

6. Agradecimentos

Este trabalho utilizou o ChatGPT da OpenAI para revisão textual e consolidação dos dados coletados.

Referências

ABNT (2012). ABNT NBR ISO/IEC 31010:2012: Gestão de riscos — Técnicas para o processo de avaliação de riscos. Technical report, Rio de Janeiro. Equivalente à ISO/IEC 31010:2012.

ABNT (2018). *ABNT NBR ISO 31000:2018 — Gestão de riscos – Diretrizes*. Associação Brasileira de Normas Técnicas, Rio de Janeiro.

ABNT (2022). ABNT NBR ISO/IEC 27001:2022 — Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos. Norma técnica, ABNT, Rio de Janeiro.

ABNT (2023). ABNT NBR ISO/IEC 27005:2023 – Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação. Equivalente à ISO/IEC 27005:2022.

Alves, R. S., Georg, M. A. C., and Nunes, R. R. (2023). Judiciário sob ataque hacker: riscos de negócio para segurança cibernética em tribunais brasileiros. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (E56):344–357.

Batista, R. R. (2022). Análise de riscos em segurança da informação: modelo integrado e simplificado de ações de segurança da informação para Instituições Federais de Ensino Superior (IFES). Dissertação de mestrado, Universidade Federal da Paraíba.

Brasil (2008). Lei nº 11.892, de 29 de dezembro de 2008 - Institui a Rede Federal de Educação Profissional, Científica e Tecnológica. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11892.htm. Acesso em 20 mai. 2025.

Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso 20 mai. 2025.

Brasil (2021). Portaria nº 713, de 8 de setembro de 2021 — Aprova o Programa de Gestão e Melhoria da Qualidade do Gasto Público no âmbito do Ministério da Educação. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-713-de-8-de-setembro-de-2021-343837861. Acesso em: 20 mai. 2025.

Brasil (2024). Decreto nº 12.069, de 21 de junho de 2024. Estratégia Nacional de Governo Digital - 2024 a 2027. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/decreto/D12069.htm. Acesso em: 19 maio 2025.

CIS (2025). CIS Critical Security Controls v8. Disponível em: https://www.cisecurity.org/controls/cis-controls-list. Acesso em: 17 mar. 2025.

CONIF, P. (2025). Conselho Nacional das Instituições da Rede Federal de Educação Profissional, Científica e Tecnológica (CONIF). Disponível em: https://portal.conif.org.br/. Acesso em: 21 mai. 2025.

Crouhy, M., Galai, D., and Mark, R. (2014). *The Essentials of Risk Management*. McGraw-Hill Education, New York, 2 edition.

CrowdStrike (2025). CrowdStrike 2025 Global Threat Report. Technical report, CrowdStrike Inc. Disponível em: https://www.crowdstrike.com/en-us/resources/reports/threat-hunting-report/. Acesso em: 02 mai. 2025.

CTIR-Gov (2025a). CTIR Gov em Números. Disponível em: https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros. Acesso em: 19 maio 2025.

CTIR-Gov (2025b). Perguntas Freqüentes ao CERT.br. Disponível em: https://www.cert.br/docs/certbr-faq.html. Acesso em: 19 maio 2025.

de Oliveira, J. L. C., de Morais Neto, H. J., de Alencar, J. C. C., da Silva, J. R., da Conceição, L. A., and Mineu, H. F. S. (2022). Matriz Orçamentária da Rede Federal de Educação Profissional, Científica e Tecnológica: Uma Ferramenta de Análise Entre a Relação Aluno Matriculado Versus Aluno Contabilizado. *Revista Foco*, 15(6):e573.

FORTI (2025). Painel de Dados do Fórum de Gestores de TIC - FORTI. Disponível em: https://portal.conif.org.br/forti. Acesso em: 31 mai. 2025.

G1 Amapá (2024). Site da UNIFAP sofre ataque hacker e fica fora do ar. Disponível em: https://g1.globo.com/ap/amapa/noticia/2024/07/23/site-da-unifap-sofre-ataque-hacker-e-fica-fora-do-ar.ghtml. Acesso em: 19 maio 2025.

G1 Mato Grosso do Sul (2023). De CPF a fotos: UFMS confirma que dados pessoais de alunos foram acessados por hackers em vazamento. Disponível em: https://x.gd/DC0Hz. Acesso em: 19 maio 2025.

G1 Paraná (2021). Site do IFPR é alvo de hackers e fica fora do ar, diz instituição. Disponível em: https://x.gd/Q05s2. Acesso em: 19 maio 2025.

G1 Piauí (2024). Site oficial da UFPI sofre invasão após ocupação da reitoria por estudantes. Disponível em: https://x.gd/CzaXn. Acesso em: 19 maio 2025.

Gonçalves, E., Bezerra da Silva, I. R., Zottmann, C. E. M., Souza Neto, J., and Nunes, R. R. (2025). Universidades sob ataque hacker: riscos de negócio para segurança cibernética em universidades brasileiras. Disponível em: https://ppee.unb.br/wp-content/uploads/2025/04/Artigo_ataque_hacker_IES_UnB.pdf. Acesso em: 10 jul. 2025.

IFTM (2025). Cadeia de Valor Institucional. https://iftm.edu.br/transparencia-prestacao-de-contas/modelo/cadeia/. Acesso em: 9 jun. 2025.

Lozada, G. and Nunes, K. S. (2018). *Metodologia científica*. SAGAH, Porto Alegre.

MGI (2023). Portaria SGD/MGI nº 852, de 28 de março de 2023. https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908. Publicada no Diário Oficial da União em 29 mar. 2023. Acesso em: 21 mai. 2025.

MGI (2025). Proposta de Cadeia de Valor da Educação para Instituições de Ensino Superior. Disponível em: https://x.gd/szQMV.

Ministério da Educação (2025). Política Nacional de Permanência (PNP). Disponível em: https://www.gov.br/mec/pt-br/pnp. Acesso em: 9 jun. 2025.

NIST (2024). The NIST Cybersecurity Framework (CSF) 2.0. Technical Report NIST CSWP 29, National Institute of Standards and Technology. Disponível em: https://doi.org/10.6028/NIST.CSWP.29. Acesso em: 19 mai. 2025.

Silva, J. D. S. (2017). Diretrizes Estratégicas de Gestão de Riscos de Segurança da Informação para Instituições Federais de Ensino Superior. Dissertação de mestrado, Universidade Federal de Pernambuco, Recife.

Souza, J. G. S., Arima, C. H., and Belda, F. R. (2020). Análise de tratamento da segurança da informação de uma instituição de ensino público federal. *Revista Ibero-Americana de Estudos em Educação*, 15(3):1309–1321. DOI: 10.21723/riaee.v15i3.13584.

Wazlawick, R. S. (2021). *Metodologia de pesquisa para ciência da computação*. LTC, Rio de Janeiro, 3 edition.