UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

JANINE LUZIA DOS SANTOS OLIVEIRA

BRING YOUR OWN DEVICE (BYOD): ESTRATÉGIAS PARA MITIGAÇÃO DE RISCOS

TOLEDO

2025

JANINE LUZIA DOS SANTOS OLIVEIRA

BRING YOUR OWN DEVICE (BYOD): ESTRATÉGIAS PARA MITIGAÇÃO DE RISCOS

Bring Your Own Device (BYOD): Risk Mitigation Strategies

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Tecnólogo em Tecnologia em Sistemas para Internet do Curso Superior de Tecnologia em Sistemas para Internet da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Fábio Engel de Camargo

TOLEDO

2025

JANINE LUZIA DOS SANTOS OLIVEIRA

BRING YOUR OWN DEVICE (BYOD): ESTRATÉGIAS PARA MITIGAÇÃO DE RISCOS

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Tecnólogo em Tecnologia em Sistemas para Internet do Curso Superior de Tecnologia em Sistemas para Internet da Universidade Tecnológica Federal do Paraná.

Data de aprovação: 18/fevereiro/2025

Fábio Engel de Camargo
Doutor em Ciência da Computação
Universidade Tecnológica Federal do Paraná

Edson Tavares de Camargo
Doutor em Ciência da Computação
Universidade Tecnológica Federal do Paraná

Alexandre Huff
Doutor em Ciência da Computação
Universidade Tecnológica Federal do Paraná

TOLEDO

2025

Dedico este trabalho ao meu estimado orientador, Prof. Dr. Fábio Engel de Camargo, que me presenteou com um tema instigante e cheio de significado. Este estudo surgiu de uma demanda pessoal de sua esposa, que inspirou sua busca por soluções técnicas para resolver o problema.

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, por me permitir chegar até aqui e concluir mais esta etapa da minha vida, concedendo-me força, sabedoria e perseverança ao longo dessa jornada.

Ao meu querido e amado esposo, Sandro, expresso minha profunda gratidão pelo apoio incondicional, paciência e compreensão durante todo este processo. Sem sua presença ao meu lado, esta conquista não teria sido possível.

À minha família, que, mesmo estando longe, sempre me apoiou e incentivou ao longo dessa jornada, compreendendo minha ausência durante este período. Minha eterna gratidão.

Ao meu orientador, Prof. Dr. Fábio Engel de Camargo, sou imensamente grata pela generosidade, paciência, dedicação e competência com que me guiou neste trabalho. Seu conhecimento e comprometimento foram essenciais para a construção deste estudo.

Aos professores membros da banca: Prof. Dr. Alexandre Huff e Prof. Dr. Edson Tavares de Camargo, pelas contribuições realizadas.

Aos demais professores que, com sua experiência e ensinamentos, contribuíram de forma significativa para minha formação acadêmica, deixo aqui meu sincero agradecimento.

Às minhas queridas amigas, Daiane e Eduarda, que compartilharam comigo essa caminhada, oferecendo apoio incondicional, incentivo e amizade, meu muito obrigada.

Por fim, agradeço a todos que, direta ou indiretamente, contribuíram para o meu crescimento profissional, pessoal e intelectual ao longo dessa jornada e, principalmente, para a realização deste trabalho.

RESUMO

Este trabalho de conclusão de curso investiga estratégias de mitigação de riscos no contexto do *Bring Your Own Device* (BYOD), analisando seus benefícios e deficiências. A pesquisa examina práticas adotadas por organizações, identificando desafios e soluções para aprimorar a segurança e o gerenciamento de riscos. Com base nesse estudo, são apresentadas recomendações para fortalecer as políticas de BYOD, considerando a evolução das ameaças digitais. Além de contribuir para o conhecimento acadêmico, a pesquisa busca influenciar práticas eficazes, fornecendo informações para profissionais, pesquisadores e gestores de segurança da informação.

Palavras-chave: segurança da informação; bring your own device (byod); gestão de dispositivos móveis; mitigação de riscos.

ABSTRACT

This study explores risk mitigation strategies in the context of Bring Your Own Device (BYOD), analyzing its benefits, challenges, and security implications. It examines organizational practices to identify key obstacles and effective solutions for enhancing risk management. Based on these findings, recommendations are proposed to strengthen BYOD policies in response to evolving digital threats. Beyond contributing to academic knowledge, this research provides insights for professionals, researchers, and information security managers, supporting the development of more effective security strategies.

Keywords: information security; bring your own device (byod); mobile device management; risk mitigation.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Nos últimos anos, a crescente propagação de dispositivos móveis e a evolução tecnológica têm transformado a maneira como as organizações abordam a gestão de dispositivos em seus ambientes de trabalho. A prática de gestão de dispositivos conhecida como “Bring Your Own Device” (BYOD), ou “traga seu próprio dispositivo”, emergiu como um fenômeno significativo, permitindo que os funcionários utilizem seus próprios dispositivos pessoais, como *smartphones*, *tablets* e *laptops*, para executar tarefas relacionadas ao trabalho. Essa prática, embora tenha o potencial de aumentar a produtividade e a flexibilidade dos funcionários, também apresenta desafios significativos relacionados à segurança da informação e ao gerenciamento de riscos.

Para Garba Jocelyn Armarego e Kenworthy (2015), essa adoção massiva do BYOD foi desencadeada por uma nova geração de funcionários que são mais experientes em tecnologia e exigem mais flexibilidade e liberdade para usar seus próprios dispositivos para realizar seu trabalho com mais precisão e rapidez.

Essa tendência reflete a necessidade de adaptação das organizações às demandas de um ambiente de trabalho em constante evolução. O BYOD é um exemplo emblemático de como a inovação tecnológica está moldando o cenário empresarial, estimulando empresas a adotar práticas mais flexíveis e modernas, o que, por sua vez, leva a um aumento significativo na produtividade e na eficiência dos funcionários, conforme pesquisa realizada pela CISCO IBSG (BRADLEY *et al.*, 2012).

Para Coto e Dias (2023), o funcionário que adota o BYOD sente-se motivado a adquirir o dispositivo que possui mais afinidade para melhor execução de suas atividades. Como resultado, há um aumento nas taxas de produtividade da empresa, bem como redução nos gastos com investimentos em compras ou atualizações de dispositivos para os funcionários.

A pandemia da COVID-19 acentuou ainda mais a adoção do BYOD por muitas organizações, quando diversas empresas adotaram o trabalho remoto como medida preventiva para conter a disseminação do vírus. Os trabalhadores precisaram equilibrar suas responsabilidades profissionais e pessoais, tornando os dispositivos móveis pessoais uma escolha conveniente. Esse cenário aumentou a necessidade de que os funcionários utilizassem seus próprios dispositivos para acessar sistemas e dados corporativos (ARAÚJO; LUA, 2021).

No entanto, para que as organizações possam realmente colher os benefícios dessa prática e alcançar os objetivos desejados, é essencial implementar medidas rigorosas que garantam a segurança e a privacidade das informações, tanto das próprias organizações quanto dos colaboradores, no contexto do BYOD.

De acordo com (RATCHFORD *et al.*, 2022), as preocupações com a segurança em relação ao BYOD têm sido alvo de discussão acadêmica desde 2012. Essa tendência pode ser atribuída ao aumento significativo no número de funcionários que acessam dados corporativos

por meio de seus dispositivos pessoais, bem como à crescente adoção desse fenômeno por diversas organizações.

A segurança da informação é uma preocupação central quando se permite que os funcionários usem seus próprios dispositivos para fins profissionais. É crucial estabelecer políticas e protocolos de segurança abrangentes que incluam a criptografia de dados, autenticação multifatorial, monitoramento de dispositivos e redes, bem como a gestão eficaz das atualizações de *software*. Além disso, a conscientização dos colaboradores sobre práticas seguras e a importância de proteger informações confidenciais é fundamental.

A privacidade dos colaboradores também deve ser cuidadosamente considerada. As políticas de BYOD devem estabelecer claramente como os dados pessoais dos funcionários são tratados, garantindo que haja uma separação nítida entre dados pessoais e informações relacionadas ao trabalho. Isso pode ser alcançado por meio de acordos de uso e, quando aplicável, soluções de gestão de dispositivos que permitam a segregação de dados.

O BYOD oferece muitos benefícios, mas é fundamental que as organizações ajam de forma responsável e proativa para assegurar que a segurança e a privacidade estejam no centro de sua estratégia de implementação. Dessa forma, será possível desfrutar das vantagens da prática do BYOD enquanto protege os ativos de informação da empresa e o direito à privacidade dos colaboradores.

À medida que o BYOD ganha popularidade nas empresas de todo o mundo, torna-se evidente que as organizações enfrentam um dilema entre aproveitar os benefícios do BYOD e mitigar os riscos associados à segurança de dados sensíveis e à privacidade dos funcionários. A flexibilidade oferecida pelo BYOD é atrativa para muitos colaboradores, que preferem usar seus próprios dispositivos para o trabalho, mas isso também expõe as empresas a vulnerabilidades potenciais, como o acesso não autorizado, perda de dispositivos e ameaças digitais. Portanto, é essencial explorar estratégias eficazes para equilibrar a produtividade e a segurança em um ambiente de BYOD.

O presente trabalho de conclusão de curso visa abordar a complexidade inerente à gestão da segurança da informação no contexto do Bring Your Own Device (BYOD). Isto porque, à medida que mais funcionários adotam dispositivos pessoais para o trabalho, as organizações enfrentam uma crescente dificuldade em garantir a proteção dos dados corporativos sensíveis e a privacidade dos colaboradores. A falta de controles adequados e a heterogeneidade dos dispositivos, sistemas operacionais e aplicativos utilizados tornam a segurança da informação uma tarefa árdua. Além disso, a gestão de riscos no contexto do BYOD também é desafiadora devido à necessidade de equilibrar a segurança com a produtividade e a satisfação dos funcionários.

Embora as organizações estejam cientes da importância da segurança e da gestão de riscos nesse cenário, muitas ainda não possuem estratégias sólidas ou não conseguem adaptá-las de forma eficaz às constantes mudanças tecnológicas e às ameaças digitais em evolução. Por este motivo, esta proposta busca realizar um estudo sobre quais são as principais defici-

ências nas abordagens de segurança atuais e quais são os principais métodos utilizados para mitigação dos riscos que essa política de segurança traz consigo.

Espera-se que este trabalho não apenas forneça uma compreensão das estratégias de mitigação de riscos no contexto do BYOD, mas também que estimule a sua adoção por parte das organizações. O resultado deste trabalho inclui uma revisão da literatura, que aborda as estratégias de segurança adotadas por organizações em ambientes de BYOD. Esse documento é um recurso atualizado, destinado a profissionais, acadêmicos e pesquisadores interessados em explorar a complexa interseção entre BYOD e segurança da informação.

Além disso, como parte do resultado, este TCC proporciona recomendações derivadas da análise das melhores práticas identificadas na literatura e nas experiências compartilhadas por profissionais do campo. Essas recomendações podem ser úteis para empresas e organizações que desejam adotar ou aprimorar suas políticas de BYOD com foco na segurança da informação. Espera-se que essas diretrizes auxiliem na tomada de decisões informadas, na implementação eficaz de estratégias de mitigação de riscos e na redução de vulnerabilidades no ambiente de BYOD.

1.1 Objetivos

Nesta sessão são apresentados os objetivos geral e específicos que regem esse trabalho.

1.1.1 Objetivo Geral

Este trabalho de conclusão de curso tem como objetivo principal estudar as estratégias de mitigação de riscos no contexto do BYOD, identificando seus principais benefícios e deficiências. Para atingir esse objetivo, é realizado um estudo sobre as principais práticas adotadas por organizações que adotam a gestão de dispositivos BYOD. Além disso, este estudo visa desenvolver recomendações práticas para aprimorar as estratégias de mitigação de riscos, levando em consideração a evolução das ameaças digitais.

Adicionalmente, este trabalho tem como objetivo fornecer um estudo que possa ser utilizado por profissionais da área de segurança da informação, gestores de TI, especialistas em gerenciamento de riscos e todos os interessados no campo da segurança da informação. Espera-se que o estudo seja útil não apenas para aqueles que desejam compreender o que é o BYOD, mas também para aqueles que buscam implementar ou aprimorar políticas de BYOD em suas organizações.

1.1.2 Objetivos Específicos

Os objetivos específicos deste trabalho incluem:

- Realizar estudo sobre estratégias de mitigação de riscos em ambientes BYOD;
- Identificar os principais benefícios e deficiências;
- Estudar as principais práticas adotadas por organizações que aderem ao BYOD;
- Desenvolver recomendações para mitigação dos riscos;
- Apresentar as principais técnicas utilizadas;
- Realizar estudo de caso na UTFPR-TD, com o intuito de investigar as estratégias e políticas existentes na instituição para mitigar os riscos associados ao BYOD.

1.2 Justificativa

O BYOD é uma tendência crescente no mundo corporativo, pois oferece uma série de benefícios para empresas e funcionários. Para as empresas, o BYOD pode reduzir custos, melhorar a produtividade e aumentar a satisfação dos funcionários. Para os funcionários, o BYOD pode proporcionar maior flexibilidade e mobilidade. O desenvolvimento tecnológico acelerado tem transformado profundamente a maneira como as organizações conduzem seus negócios. A adoção de práticas em constante evolução, como o BYOD, é um exemplo claro dessa mudança que, tem como propósito impulsionar uma produtividade e eficiência cada vez mais ampliadas no ambiente de trabalho.

À medida que a tecnologia avança a passos largos, as empresas estão reavaliando suas abordagens e estratégias para permanecerem competitivas no mercado. A integração do BYOD é uma resposta a esse desafio, permitindo que os funcionários usem seus próprios dispositivos, para realizar tarefas relacionadas ao trabalho. Isso não apenas oferece maior flexibilidade, mas também ajuda a aprimorar a eficiência e a produtividade, uma vez que os colaboradores podem trabalhar da forma que considerarem mais conveniente.

Estudos recentes tem demonstrado que à adesão ao BYOD, tem um impacto positivo nos resultados das organizações. Por exemplo, um estudo realizado por (COTO; DIAS, 2023) afirma que o funcionário que adota o BYOD, adquire um dispositivo eletrônico que possui maior afinidade e melhora a execução de suas atividades. Como resultado sobem as taxas de produtividade da empresa ao mesmo tempo que reduz seus investimentos em compras ou atualizações desses equipamentos.

Apesar dos benefícios do BYOD, existem também alguns desafios associados a essa prática, como a segurança dos dados e a conformidade com as leis de privacidade. O objetivo

deste estudo é analisar os desafios associados ao BYOD e apresentar soluções para mitigá-los, baseado em recomendações de melhores práticas.

1.3 Estrutura do trabalho

Este trabalho está estruturado da seguinte forma: o Capítulo 2 apresenta os conceitos fundamentais relacionados ao tema de estudo, essenciais para a compreensão do conteúdo. No Capítulo 3, são explorados trabalhos relacionados ao BYOD que contribuíram para o desenvolvimento deste texto. O Capítulo 4 descreve os procedimentos metodológicos empregados para alcançar os objetivos propostos. No Capítulo 5, é relatado um estudo de caso realizado na Universidade Tecnológica Federal do Paraná, Campus Toledo, com o intuito de verificar a existência de diretrizes institucionais sobre a política de BYOD. O Capítulo 6 apresenta recomendações destinadas a organizações interessadas na implementação da prática de BYOD. Por fim, o Capítulo 7 reúne as conclusões obtidas ao longo do trabalho.

2 REFERENCIAL TEÓRICO

No presente capítulo, são delineadas as bases teóricas e conceituais referentes à gestão de riscos no contexto da segurança da informação, especificamente no âmbito do ambiente BYOD. São expostos os princípios fundamentais cruciais para assegurar a confidencialidade, integridade e disponibilidade da informação, bem como as principais estratégias para mitigação de riscos. Com isso, pretende-se proporcionar ao leitor uma compreensão abrangente das fundamentações teóricas que orientam esta pesquisa, estabelecendo, assim, um alicerce robusto para a construção do arcabouço que fundamentará as fases subsequentes deste estudo.

2.1 Segurança da Informação

De acordo com a ISO/IEC... (2005), a informação é um ativo valioso e, portanto, é essencial para a continuidade dos negócios de uma organização que ela seja adequadamente protegida. A incessante evolução das Tecnologias de Informação e Comunicação (TICs) tem redefinido o panorama empresarial contemporâneo, tornando-o progressivamente dinâmico e interconectado. Diante dessa conjuntura em constante transformação, emerge a necessidade urgente de conceber estratégias voltadas à garantia da continuidade operacional das organizações. Nesse contexto, os sistemas de informação surgem como instrumentos fundamentais para subsidiar as atividades de gestão, viabilizando o processamento eficiente das informações e proporcionando agilidade na tomada de decisões. Esses sistemas desempenham um papel crucial para assegurar a sustentabilidade e competitividade organizacional em um ambiente digital em constante evolução.

De acordo com a IBM (2024), a segurança da informação é um conjunto de medidas e práticas adotadas para salvaguardar informações de relevância para uma organização, englobando desde documentos em formato físico até dados digitais. Essas medidas visam proteger tais informações contra acessos não autorizados, divulgações indevidas, alterações não autorizadas e usos não permitidos. A implementação da segurança da informação se fundamenta em princípios estabelecidos há décadas e sujeitos a uma evolução contínua, delineando diretrizes para assegurar a integridade e confiabilidade dos sistemas de informação, ao mesmo tempo em que se busca reduzir os riscos associados a esses ambientes digitais. Esta abordagem abrange não apenas a proteção dos ativos digitais, como *hardware* e *software*, mas também se estende à proteção das pessoas envolvidas em todas as etapas do ciclo de vida da informação dentro da infraestrutura de tecnologia da informação (TI) da empresa, incluindo produção, armazenamento, uso e troca de dados.

Ainda segundo a IBM (2024), o aumento do uso de dispositivos pessoais em ambientes corporativos tem gerado preocupações sobre segurança. Para melhorar a política BYOD, é essencial solicitar que funcionários instalem *softwares* de segurança e ampliar o controle centralizado. Além disso, promover uma cultura organizacional que valorize a segurança, incentivando

práticas como senhas fortes, autenticação multifatorial e atualizações de *software*, juntamente com a criptografia de dados, pode ser fundamental para mitigar os riscos associados ao BYOD. Uma estratégia abrangente de segurança de dados incorpora pessoas, processos e tecnologias. Independentemente da localização de armazenamento dos dados, seja em ambiente local, em data center empresarial ou na nuvem pública, é imprescindível assegurar que as instalações estejam devidamente protegidas contra invasões, bem como disponham de medidas adequadas de prevenção e combate a incêndios, além de sistemas eficientes de climatização.

A ISO/IEC... (2005), define inicialmente a segurança da informação como: "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio". A norma ressalta ainda que, a segurança da informação é alcançada mediante a adoção de um conjunto apropriado de medidas de controle, que englobam políticas, procedimentos, processos, estruturas organizacionais, bem como elementos de *software* e *hardware*. Tais controles devem ser estabelecidos, implementados, monitorados, revisados criticamente e aprimorados, conforme necessário, visando assegurar a realização dos objetivos tanto do negócio quanto da segurança da organização. É recomendável que essas ações sejam integradas aos demais processos de gestão empresarial.

Segundo Dorneles, Rohden e Telocken (2021), diante da crescente sofisticação dos ataques cibernéticos, é fundamental que as empresas estejam atentas à adoção de soluções de segurança. Essa postura proativa se mostra essencial para prevenir os perigos decorrentes da Internet e proteger os pontos de extremidade da rede corporativa. Portanto, é possível conceituar segurança da informação como o domínio de estudo dedicado à salvaguarda das informações contra ameaças que possam comprometer sua integridade, disponibilidade e confidencialidade, visando assegurar a continuidade operacional das organizações e reduzir os riscos envolvidos.

De acordo com Barbosa, Barriviera *et al.* (2016), o objetivo primordial da segurança da informação reside na minimização dos diversos riscos concernentes à divulgação não autorizada de dados, sendo que, frequentemente, a maior fonte de perigo pode emergir internamente na organização. Nesse sentido, é imprescindível a adoção de um conjunto abrangente de assuntos, procedimentos e ferramentas a fim de garantir a mais eficiente proteção possível para as informações.

Para Almeida (2023), a popularização da Internet e a disseminação de diversas tecnologias tem transformado de forma significativa a sociedade contemporânea. Essa evolução trouxe consigo novas formas de interação social e econômica, que vieram acompanhadas de novos desafios e dilemas inéditos até então. Entre esses desafios, destaca-se a crescente incidência de crimes cibernéticos, que vêm se tornando cada vez mais frequentes e sofisticados. Já de acordo com Oliveira *et al.* (2016), indivíduos com intenções maliciosas, utilizando-se de meios fraudulentos, exploram vulnerabilidades das organizações, resultando em desordem, danos mo-

netários e comprometimento da reputação corporativa, acarretando prejuízos substancias às entidades empresariais.

De acordo com Fontes, Balloni e Laudon (2015), a segurança dos sistemas de informação deve contemplar não só os aspectos técnicos como também os sociais, relacionados ao ambiente organizacional e às pessoas. Ressaltando que o desempenho da segurança de um sistema de informação deve levar em conta: os aspectos sociais como a conscientização, treinamento, bem como deve considerar a situação dos colaboradores, como estabilidade financeira, segurança de moradia e estrutura familiar; e os aspectos técnicos referentes a tecnologia e aos recursos tecnológicos fundamentais para a proteção da informação contra vulnerabilidades existentes. O que cumina no desenvolvimento de soluções sociotécnicas que combinam eficiência técnica com necessidades humanas e organizacionais que elevam a produtividade.

Segundo a perspectiva de Soomro, Shah e Ahmed (2016), as pessoas são o elemento mais crítico na gestão de segurança da informação, podendo apresentar aspectos negativos como estar envolvidos em roubo de informações e violação de política de aceso o que representa uma grande ameaça para as organizações empresariais. No entanto, por outro lado, se o funcionário estiver alinhado com a política de segurança, a conscientização e o treinamento adequado terão um impacto positivo significativo na segurança das informações. Tal como indicado por Ratchford *et al.* (2022), a organização precisa garantir que o usuário compreenda, concorde e assine as políticas relevantes contra os riscos relacionados ao BYOD, antes que a atividade seja permitida.

2.1.1 Pilares da segurança da informação

A segurança da informação repousa sobre três pilares fundamentais, conhecidos como a tríade da segurança da informação. Esses pilares são a base para o desenvolvimento de estratégias eficazes que visam proteger os ativos de informação de uma organização. A tríade é composta pelos seguintes aspectos: a confidencialidade, a integridade e a disponibilidade (CID). A ISO/IEC... (2012), define a segurança cibernética como preservação da confidencialidade, integridade, e da disponibilidade da informação no espaço cibernético. Já a ISO/IEC... (2005), descreve a segurança da informação como a preservação da confidencialidade, da integridade e da disponibilidade da informação; e adicionalmente reforça que, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem estar envolvidas como parte da segurança da informação.

A confidencialidade é o primeiro pilar da segurança da informação e refere-se à proteção das informações contra acessos não autorizados. Conforme Hintzbergen *et al.* (2018), a confidencialidade é um princípio fundamental da segurança da informação que se refere à garantia de que a informação não seja acessada ou revelada a pessoas, entidades ou processos não autorizados, garantindo que apenas indivíduos autorizados tenham acesso às informações relevantes. Garantir a confidencialidade implica em adotar medidas que restrinjam o acesso apenas

a usuários autorizados. Isso pode envolver a implementação de controles de acesso, criptografia e políticas de classificação de dados. As organizações buscam preservar a confidencialidade para proteger informações sensíveis, como dados financeiros, estratégias de negócios e informações pessoais (STAPLETON, 2014).

A integridade é o segundo pilar da segurança da informação e está relacionada à garantia de que as informações permaneçam precisas e íntegras ao longo do tempo. Os dados não devem ser alterados de forma não autorizada, seja por erro acidental ou manipulação maliciosa. Para assegurar a integridade, são implementados mecanismos de controle, como verificações de *checksum*, assinaturas digitais e sistemas de controle de versões. Manter a integridade é crucial para garantir a confiabilidade das informações e evitar decisões ou ações baseadas em dados corrompidos. Para Hintzbergen *et al.* (2018), a integridade visa proteger a precisão e a consistência dos ativos. Garantindo que modificações não autorizadas não sejam realizadas no *software* e no *hardware*, evitando alterações não autorizadas nos dados por pessoal autorizado ou não autorizado, bem como processos. Além disso, a integridade assegura que os dados permaneçam consistentes tanto internamente quanto externamente

O terceiro pilar, a disponibilidade, diz respeito à garantia de que as informações estejam acessíveis quando necessário. Isso implica em prevenir e mitigar eventos que possam causar interrupções nos sistemas, como ataques de negação de serviço (*Denial of Service* - DoS), falhas de *hardware* ou desastres naturais. A disponibilidade é essencial para manter a continuidade dos negócios, assegurando que os usuários possam acessar informações críticas quando precisarem. Estratégias como *backups* regulares, redundância de sistemas e planos de recuperação de desastres são essenciais para garantir a disponibilidade. Conforme Hintzbergen *et al.* (2018), a disponibilidade é uma característica fundamental na segurança da informação, referindo-se à capacidade dos sistemas e recursos de estar prontamente acessíveis e utilizáveis quando necessários por entidades autorizadas.

Em sua essência, autenticidade refere-se à qualidade de ser genuíno, legítimo e confiável. No contexto da informação digital, a autenticidade envolve duas dimensões interrelacionadas: a autenticidade das informações e a autenticidade dos usuários. A primeira diz respeito à garantia de que as informações são provenientes de fontes confiáveis e não foram adulteradas ou manipuladas. Já a segunda dimensão refere-se à validação das identidades dos usuários, assegurando que são quem afirmam ser. A International Organization for Standardization (ISO) (2018), define a autenticidade como a propriedade de que uma entidade é o que afirma ser. Para garantir a autenticidade das informações, é fundamental implementar estratégias robustas que visem garantir a autenticidade das informações e dos usuários. Isso pode incluir a verificação da fonte das informações, a adoção de métodos de criptografia para proteger a integridade dos dados, e a implementação de políticas de autenticação robustas, como senhas seguras e autenticação de dois fatores. Além disso, a educação e conscientização dos usuários sobre os riscos de informações falsas e a importância da verificação da autenticidade das informações são medidas essenciais na promoção de uma cultura de segurança digital.

Conforme Hintzbergen *et al.* (2018), a responsabilidade é a atribuição de ações e decisões de um entidade. A ISO/IEC... (2005), aborda de forma abrangente e sistemática a necessidade de estabelecer responsabilidades claras e garantir que todas as partes interessadas assumam sua parcela de responsabilidade na gestão da segurança da informação. A norma ressalta ainda que, a organização precisa ainda estar ciente, de que em caso de terceirização a responsabilidade final pela informação processada por um parceiro de terceirização permanece com a organização. O princípio da responsabilidade implica que, cada pessoa ou entidade envolvida em qualquer aspecto do ciclo de vida da informação deve entender suas responsabilidades específicas em relação à segurança da informação e agir de acordo com elas. Isso pode incluir a implementação de políticas de segurança, a adoção de práticas seguras de manuseio de dados, a realização de treinamento regular em segurança da informação e a participação ativa na proteção dos ativos de informação.

A International Organization for Standardization (ISO) (2018), afirma que o princípio do não repúdio desempenha um papel crucial na segurança da informação, referindo-se à habilidade de estabelecer evidências que comprovem a ocorrência de um evento ou ação, juntamente com suas entidades de origem. No contexto da segurança da informação, é essencial garantir que as transações e interações digitais sejam adequadamente registradas e autenticadas, a fim de prevenir disputas ou negações posteriores por parte das partes envolvidas. O não repúdio é fundamental para garantir a integridade e a confiabilidade das informações em ambientes digitais, proporcionando uma base sólida para a auditoria, a conformidade regulatória e a resolução de disputas. Ao implementar mecanismos de não repúdio, como assinaturas digitais e registros de transações imutáveis, as organizações podem fortalecer sua postura de segurança e mitigar os riscos associados à negação de eventos críticos.

Para Hintzbergen *et al.* (2018), a confiabilidade diz respeito a propriedade de consistência dos comportamentos e resultados desejados. O princípio da confiabilidade na segurança da informação destaca a importância de estabelecer e manter controles de segurança que sejam confiáveis, consistentes e eficazes para proteger os ativos de informação contra uma ampla gama de ameaças e vulnerabilidades. Segundo a ISO/IEC... (2005), mudanças em sistemas operacionais apenas devem ser realizadas quando houver uma razão de negócio válida para tal, como um aumento no risco do sistema. A atualização de sistemas às versões mais atuais de sistemas operacionais ou aplicativos nem sempre é do interesse do negócio, pois pode introduzir mais vulnerabilidades e instabilidades ao ambiente do que a versão corrente. Pode haver ainda a necessidade de treinamento adicional, custos de licenciamento, suporte, manutenção e sobrecarga de administração, bem como a necessidade de novos equipamentos, especialmente durante a fase de migração. Ademais, os controles de segurança devem ser aplicados de forma consistente ao longo do tempo, independentemente de mudanças nos sistemas, processos ou ambientes operacionais, uma vez que tais mudanças podem trazer impactos a confiabilidade das aplicações.

Os princípios fundamentais da segurança da informação operam de maneira interligada e complementar. Uma abordagem equilibrada e abrangente desses pilares é crucial para estabelecer uma postura de segurança robusta. Ao se concentrar nos elementos de confidencialidade, integridade, disponibilidade, autenticidade, responsabilidade, não repúdio e confiabilidade, as organizações podem desenvolver estratégias de segurança que protegem de forma eficaz seus ativos de informação contra uma ampla gama de ameaças. Essa abordagem abrangente é essencial para promover a sustentabilidade e a confiança em um ambiente digital dinâmico e em constante evolução, garantindo não apenas a segurança dos dados, mas também a autenticidade das transações realizadas, a responsabilização pelas ações tomadas, a impossibilidade de negar a autoria de uma ação e a confiabilidade dos sistemas e processos de segurança implementados. Portanto, ao adotar uma visão holística que englobe todos esses princípios, as organizações podem fortalecer significativamente sua postura de segurança e mitigar os riscos associados à crescente complexidade das ameaças cibernéticas.

2.2 Gerenciamento de Riscos

De acordo com Kim e Solomon (2014), risco é a possibilidade de que uma ameaça em particular exponha uma vulnerabilidade que possa prejudicar uma organização. Os autores ressaltam ainda que, a extensão do dano que uma ameaça pode causar determina o nível do risco. Já para Hintzbergen *et al.* (2018), um risco é a probabilidade de um agente ameaçador tirar vantagem de uma vulnerabilidade e o correspondente impacto nos negócios. Ele afirma que, se um sistema de detecção de intrusão não for implementado na rede, haverá maior probabilidade de um ataque não ser percebido até que seja tarde demais. Nesse sentido, ele afirma que o risco amarra a vulnerabilidade, a ameaça e a probabilidade de exploração ao impacto resultante nos negócios.

Segundo Kim e Solomon (2014), ativos, vulnerabilidades e ameaças são elementos constituintes do risco, formando partes integrantes de um sistema complexo, em vez de uma simples fórmula. Os ativos podem tanto aumentar quanto diminuir seu valor ao longo do tempo. É crucial adotar procedimentos proativos para detectar e remediar vulnerabilidades, garantindo a segurança dos ativos. Além disso, novas ameaças continuam a surgir, adicionando-se às já existentes, o que requer uma constante vigilância e adaptação. Consequentemente, à medida que esses fatores sofrem alterações ao longo do tempo, o próprio risco também se modifica, exigindo reavaliações periódicas para identificar e abordar novas fontes de risco emergentes.

Conforme a (ABNT) (2018), a gestão de riscos são atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos. No cenário empresarial atual, organizações de todos os tipos e tamanhos estão sujeitas a uma infinidade de influências e fatores, tanto internos quanto externos, que podem afetar significativamente sua capacidade de alcançar objetivos estabelecidos. Nesse contexto, o gerenciamento de riscos surge como uma prática essencial e iterativa da governança corporativa, fundamental para a tomada de decisões mais

informadas e estratégicas, auxiliando as organizações a proteger seus ativos, otimizar suas operações e alcançar seus objetivos de negócios de forma mais eficaz.

Na perspectiva de Konzen *et al.* (2013), as atividades das organizações frequentemente enfrentam riscos, o que significa que essas organizações devem lidar com esses riscos de forma proativa. Isso envolve identificar, analisar, avaliar e decidir se os mesmos devem ser tratados ou não. Esse processo de identificação, análise e avaliação leva a decisões estratégicas, onde a organização, ao identificar um risco, avalia o quão significativo é o impacto desse risco e com que frequência ele pode ocorrer.

A (ABNT) (2018), afirma que o propósito da gestão de riscos é a criação e proteção de valor. Ela melhora o desempenho, encoraja a inovação e apoia o alcance de objetivos. Já de acordo com Kim e Solomon (2014), a finalidade do gerenciamento de risco é reduzir o risco para níveis toleráveis. Ele afirma ainda que, quase nunca um será possível eliminar um risco por completo. E que após a identificação de uma cultura de risco em uma organização é necessário avalia-los e então reduzir aqueles que possam ter um maior efeito sobre a organização.

É fundamental entender que a gestão de riscos não é uma atividade separada, mas sim uma parte integrante de todas as atividades e processos de uma organização. Desde a concepção de estratégias até a realização de tarefas diárias, a gestão de riscos está presente em todos os aspectos da estrutura organizacional. Essa abordagem abrangente não apenas melhora a capacidade da organização de reconhecer e reduzir possíveis ameaças, mas também cultiva uma cultura de responsabilidade e conscientização sobre riscos em todos os níveis da hierarquia. Segundo a (ABNT) (2018), o gerenciamento de riscos considera os contextos externo e interno da organização, incluindo o comportamento humano e os fatores culturais que influenciam significativamente todos os aspectos da gestão de riscos em cada nível e estágio.

2.2.1 Princípios da gestão de riscos

De acordo com (ABNT) (2018), os princípios são a base para gerenciar riscos e convém que sejam considerados quando se estabelecerem a estrutura e os processos de gestão de riscos da organização. Eles fornecem orientações sobre as características da gestão de riscos eficaz e eficiente, comunicando seu valor e explicando sua intenção e propósito. Convém que estes princípios possibilitem uma organização a gerenciar os efeitos da incerteza nos seus objetivos. A Figura 1 apresenta os princípios citados na (ABNT) (2018), que fornecem características primordiais para uma gestão de riscos eficiente, os quais são essenciais para uma abordagem eficaz na identificação, avaliação e tratamento dos riscos em uma organização.

Para implementar uma gestão de riscos eficaz, é necessário incorporar os elementos ilustrados na Figura 1. Isso pode ser explicado da seguinte maneira:

- Integrada, onde a gestão de riscos é parte integrante de todas as atividades organizacionais.

Figura 1 – Princípios do gerenciamento de riscos.

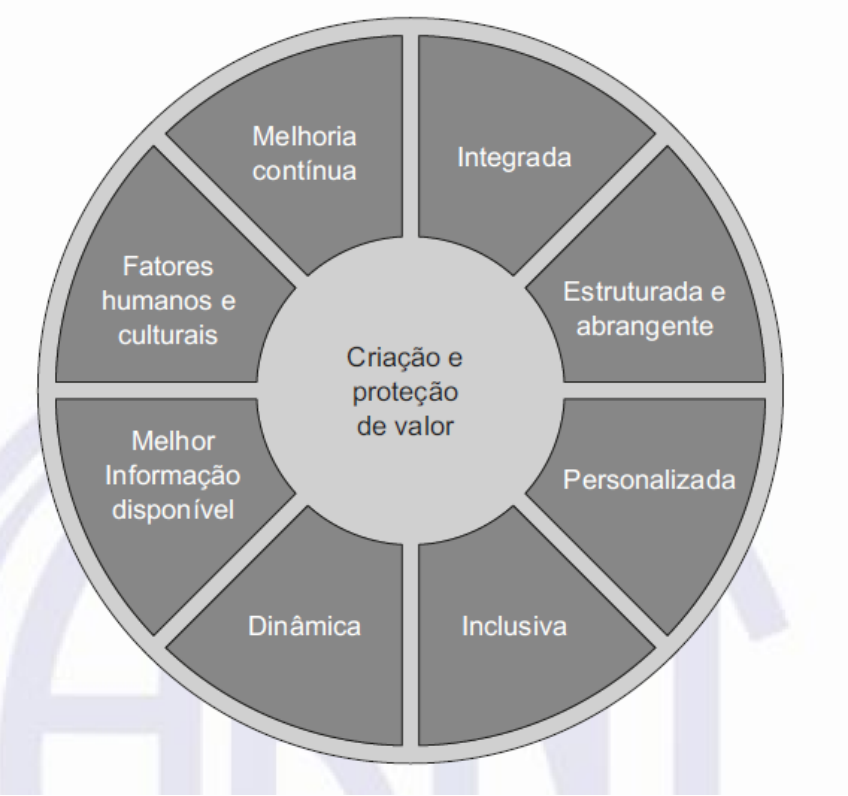

Figura reproduzida a partir de ((ABNT), 2018).

- Estruturada e abrangente, é uma abordagem de gestão de riscos que contribui para resultados consistentes e comparáveis.
- Personalizada, nessa estrutura o processo de gestão de riscos são personalizados e proporcionais aos contextos externo e interno da organização relacionados aos seus objetivos.
- Inclusiva, nessa estrutura o envolvimento apropriado e oportuno das partes interessadas possibilita que seus conhecimentos, pontos de vista e percepções sejam considerados. Isto resulta em melhor conscientização e gestão de riscos fundamentada.
- Dinâmica, nessa estrutura os riscos podem emergir, mudar ou desaparecer à medida que os contextos externo e interno de uma organização mudem. A gestão de riscos antecipa, detecta, reconhece e responde a estas mudanças e eventos de uma maneira apropriada e oportuna.
- Melhor informação disponível, nessa estrutura as entradas para a gestão de riscos são baseadas em informações históricas e atuais, bem como em expectativas futuras. A gestão de riscos explicitamente leva em consideração quaisquer limitações e incertezas associadas a estas informações e expectativas. É necessário que a informação seja oportuna, clara e disponível para as partes interessadas pertinentes.

- Fatores humanos e culturais, nessa estrutura o comportamento humano e a cultura influenciam significativamente todos os aspectos da gestão de riscos em cada nível e estágio.
- Melhoria contínua, nessa estrutura a gestão de riscos é melhorada continuamente por meio do aprendizado e experiências.

2.2.2 Processo de gestão de riscos

Segundo as diretrizes da (ABNT) (2018), o processo de gestão de riscos compreende a implementação organizada de políticas, métodos e procedimentos de gerenciamento destinados às etapas de comunicação, consulta, contextualização, bem como na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos. Esse processo é formado por um conjunto de componentes que estabelecem os fundamentos e os arranjos organizacionais necessários para lidar com os possíveis riscos que as organizações podem vir a enfrentar, promovendo assim uma abordagem pró-ativa e sistemática para a gestão de riscos empresariais.

O processo da gestão de riscos deve ser parte integrante da gestão, incorporado na cultura e nas práticas das organizações e adaptados aos processos de negócios da organização. A gestão envolve atividades para dirigir, controlar e melhorar continuamente a organização dentro de estruturas apropriadas. Essas atividades incluem o ato, a maneira ou a prática de organizar, manusear, dirigir, supervisionar e controlar recursos. A Figura 2 ilustra o processo da gestão de riscos, que terá suas etapas descritas a seguir.

A etapa de comunicação e consulta na avaliação de riscos, conforme definida pela (ABNT) (2018) é essencial para uma gestão eficaz de riscos empresariais. Envolve a troca de informações entre partes interessadas internas e externas, bem como a busca ativa por perspectivas diversas sobre os riscos identificados. A comunicação clara e transparente garante que todos compreendam os riscos e as medidas de mitigação propostas, enquanto a consulta aproveita o conhecimento das partes interessadas para enriquecer o processo de avaliação de riscos. Essa abordagem colaborativa promove uma gestão abrangente e eficaz dos riscos organizacionais.

De acordo com a (ABNT) (2018), na etapa escopo, contexto e critérios na avaliação de risco ocorre a definição do escopo da avaliação, delimitando as áreas ou processos a serem avaliados. Simultaneamente, estabelece-se o contexto organizacional, que engloba objetivos, partes interessadas, ambiente interno e externo, influências culturais e regulamentares. Os critérios de avaliação são estabelecidos para orientar a identificação, análise e avaliação dos riscos, abrangendo aspectos como tolerância ao risco, impacto nos objetivos organizacionais e conformidade legal. Esta etapa fornece uma base sólida para o desenvolvimento de estratégias de gestão de riscos, assegurando o alinhamento do processo com os objetivos da organiza-

Figura 2 – Processo de gestão de riscos

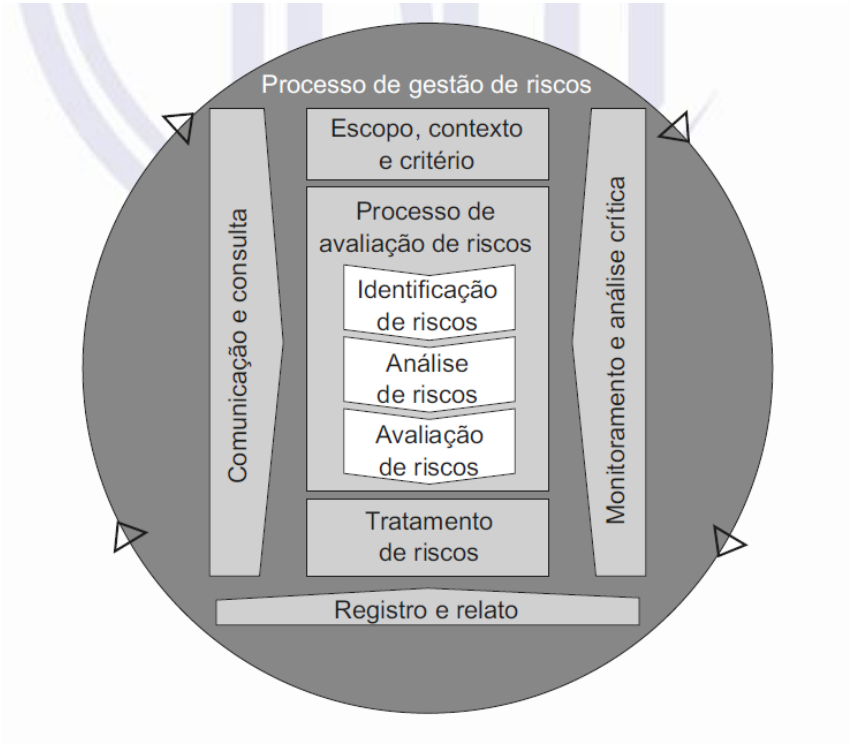

Figura reproduzida a partir de ((ABNT), 2018).

ção e a consideração abrangente dos fatores que podem influenciar os riscos enfrentados pela empresa.

O processo de avaliação de riscos deve ser conduzido de forma sistematizada, iterativa, colaborativa e utilizando-se de informações confiáveis para uma gestão eficaz dos riscos organizacionais. De acordo com a norma (ABNT) (2018), esses princípios ajudam as organizações a identificar, analisar e avaliar os riscos de forma abrangente e a implementar medidas adequadas para mitigar seu impacto negativo, conforme descritos nas etapas a seguir:

- Identificação de riscos, nessa etapa, a organização mapeia os riscos potenciais que podem afetar seus objetivos, utilizando diversas técnicas como *brainstorming*, análise de histórico, análise SWOT (*Strengths, Weaknesses, Opportunities and Threats*) e pesquisas. Os riscos identificados são documentados de forma clara e concisa, incluindo sua descrição, categoria, causas potenciais e consequências. Segundo as diretrizes da (ABNT) (2018), para a identificação de riscos, as organizações devem obter uma visão abrangente das ameaças e oportunidades que podem impactar seus negócios, permitindo uma tomada de decisão mais consciente, proativa e eficaz.

- Análise de riscos, essa etapa consiste em compreender a natureza e o potencial impacto de cada risco nos objetivos da organização. Isso envolve considerar de forma detalhada a probabilidade do risco se concretizar, através de fatores históricos, o contexto atual e as tendências. Envolve avaliar o impacto e consequências do risco, tanto positivas quanto negativas. Envolve ainda determinar o nível de incerteza associado

ao risco, reconhecendo a dificuldade em prever eventos futuros com total precisão. A análise pode ser qualitativa ou quantitativa, dependendo do propósito da análise, da disponibilidade e confiabilidade da informação, e dos recursos disponíveis.

- Avaliação de riscos, nessa etapa a organização obtém uma visão abrangente da severidade de cada risco, ou seja, do impacto potencial que ele pode causar nos objetivos da organização permitindo a tomada de decisões estratégicas e a alocação eficiente de recursos para mitigar os riscos mais críticos e proteger seus objetivos. A avaliação de riscos é um processo contínuo que deve ser revisado periodicamente para refletir as mudanças no contexto da organização e no ambiente externo.

Segundo a (ABNT) (2018), a etapa de tratamento de riscos é onde são definidas as ações para minimizar as ameaças e proteger os objetivos das organizações. As ações implementadas devem ser monitoradas, revisadas e adaptadas periodicamente para refletir as mudanças no contexto da organização e no ambiente externo. No contexto do tratamento de riscos é imprescindível a comunicação das ações de tratamento de riscos para as partes interessadas relevantes, garantindo seu engajamento e total compreensão. As opções para tratar o risco podem envolver um ou mais dos seguintes aspectos:

- Evitar o risco ao decidir não iniciar ou continuar com a atividade que dá origem ao risco;
- Assumir ou aumentar o risco de maneira a perseguir uma oportunidade;
- Remover a fonte de risco;
- Mudar a probabilidade;
- Mudar as consequências;
- Compartilhar o risco (por exemplo, por meio de contratos, compra de seguros);
- Reter o risco por decisão fundamentada.

Por fim, a etapa de monitoramento e análise crítica na gestão de riscos, conforme definida pela (ABNT) (2018), é essencial para garantir a eficácia contínua do sistema de gestão de riscos de uma organização. Ao acompanhar regularmente o desempenho, analisar criticamente os resultados e envolver as partes interessadas, com isso a organização pode identificar áreas de melhoria e tomar medidas proativas para mitigar riscos e promover uma cultura de gestão de riscos eficaz. Desta maneira, pode-se afirmar que gestão de riscos não é uma evento único, mas sim um processo contínuo que deve ser integrado à cultura e aos processos da organização, revisado periodicamente para garantir sua efetividade e relevância em um ambiente em constante evolução.

2.3 Dispositivos Móveis

Para o NIST (2013), os dispositivos móveis não são mais novidade no local de trabalho. Os dispositivos móveis são essencialmente plataformas de computação de uso geral. Eles não estão restritos à execução de uma operação e podem, em vez disso, ser usados em muitos domínios diferentes, incluindo médico, industrial e de entretenimento. Já de acordo com o NIST (2020), um dispositivo móvel é um dispositivo de computação que possui um formato pequeno, de modo que pode ser transportado por um único indivíduo; foi projetado para operar sem conexão física; possui armazenamento de dados local, não removível ou removível; e inclui uma fonte de energia independente. As funcionalidades do dispositivo móvel também pode incluir capacidades de comunicação de voz, sensores integrados que permitem ao dispositivo capturar informações e/ou recursos integrados para sincronizar dados locais com locais remotos.

Os dispositivos móveis modernos, evoluíram de simples ferramentas de comunicação para poderosas plataformas de computação de uso geral e transformaram significativamente o cenário empresarial. A mobilidade oferecida por esses dispositivos revolucionou a forma como as organizações fornecem serviços de tecnologia da informação e realizam suas operações. No entanto, esse avanço não vem sem desafios, especialmente em relação à segurança da informação.

Desenvolvidos inicialmente para o uso pessoal, os dispositivos móveis se tornaram peças-chave nas engrenagens das empresas. Ao lidarem com informações confidenciais, esses aparelhos se transformaram em alvos convidativos para ataques cibernéticos. As organizações, embora cientes dos benefícios em produtividade e agilidade na tomada de decisões que os dispositivos móveis oferecem, também estão cada vez mais conscientes das ameaças específicas que eles representam.

A adoção cada vez maior de tecnologias móveis por consumidores e empresas moldou um novo cenário de ameaças. Isso se manifesta em um crescimento exponencial de *malwares* e vulnerabilidades que afetam desde o dispositivo individual até os aplicativos, redes e infraestrutura de gerenciamento relacionados. A natureza diversificada e em constante evolução do cenário dos dispositivos móveis apresentam dificuldades significativas para a seleção, integração e gerenciamento dessas tecnologias em ambientes corporativos.

Para mitigar os riscos associados ao uso de dispositivos móveis, as empresas devem implementar políticas e infraestruturas de segurança robustas. Isso inclui a proteção de dispositivos, aplicativos, conteúdos e acessos por meio de medidas como autenticação multifatorial, criptografia de dados e implementação de soluções de gerenciamento de dispositivos móveis (*Mobile Device Management* - MDM) e de gerenciamento de aplicativos móveis (*Mobile Application Management* - MAM).

É importante ressaltar que os dispositivos móveis demandam proteções adicionais devido à sua portabilidade e uso comum fora do perímetro de rede das organizações. Enquanto as tecnologias de gerenciamento de *laptops* estão convergindo com aquelas de dispositivos

móveis, as soluções de segurança disponíveis para cada tipo de dispositivo ainda diferem significativamente. Além disso, os dispositivos móveis frequentemente possuem recursos únicos, como múltiplas interfaces de rede sem fio e sensores integrados, que os tornam mais suscetíveis a ameaças.

3 TRABALHOS RELACIONADOS

O *Bring Your Own Device* (BYOD) emerge como um fenômeno que moldou significativamente o panorama contemporâneo da tecnologia e da gestão empresarial. O conceito ganhou proeminência na última década, sendo objeto de considerável pesquisa acadêmica. O advento do BYOD remonta aos anos 2000, com a crescente inserção de dispositivos móveis no ambiente corporativo. Desde então, pesquisadores têm se dedicado a examinar os impactos, desafios e benefícios associados à implementação do BYOD. O auge das investigações sobre BYOD ocorreu na primeira metade da década de 2010, quando a tendência atingiu sua maturidade e se consolidou como uma prática comum em muitas organizações (RATCHFORD *et al.*, 2022). As pesquisas abordam questões cruciais, como segurança da informação, gestão de riscos, aspectos legais e impacto na produtividade. À medida que as dinâmicas do trabalho continuam a evoluir, a pesquisa acadêmica sobre BYOD permanece vital para compreender e enfrentar os desafios contemporâneos associados à integração eficaz de dispositivos pessoais no ambiente de trabalho. A seguir são apresentados resumos de trabalhos significativos no contexto de BYOD.

O trabalho de Ratchford *et al.* (2022) apresenta uma lista de artigos que fazem uma revisão sistemática sobre o tema. O estudo identifica os problemas de segurança do BYOD e classifica-os baseando-se em uma abordagem holística de segurança, identificando os problemas e associando-os aos domínios organizacionais referentes à administração, à tecnologia da informação, aos usuários e aos dispositivos móveis pessoais. No domínio de gerenciamento foram identificados problemas frequentes de governança, políticas e gerenciamento de riscos. Quanto ao domínio de TI foram identificados problemas relacionados a rede, às políticas, ao gerenciamento de riscos e implementação de práticas recomendadas. Já no domínio de usuário identificou-se questões relacionadas à conformidade, ao comportamento do usuário e a privacidade dos usuários. No domínio de dispositivo móvel identificou-se questões relacionadas a segurança do dispositivo em geral, à segregação de dados e ao *malware*.

Como resultado dessa revisão foram identificados 22 problemas de segurança em ambientes BYOD. O estudo classificou os problemas encontrados em cada domínio. Os resultados apontaram que 86% dos artigos revisados atribuíram problemas e considerações de segurança ao domínio de TI, 51% dos problemas de segurança atribuídos ao domínio de gerenciamento, 45% atribuíram problemas de segurança ao domínio de usuários e 19% relacionaram problemas ao domínio de dispositivos móveis. Ainda de acordo com os resultados, entre as preocupações abordadas com maior frequência estão as políticas de segurança BYOD, políticas de segurança de rede, as políticas de proteção de dados, as políticas de comportamento do usuário e as políticas de governança.

Também observou-se questões de segurança pouco discutidas, mas que também representam preocupações, como tópicos referentes as considerações legais, dentre outros. Ainda de acordo com o estudo os problemas de segurança do BYOD podem estar associados a mais

de um domínio, como por exemplo os problemas associados à educação que envolvem treinamento, e conscientização estão relacionados aos domínios de gerenciamento, TI e usuário o que ressalta à necessidade de interação entre esses domínios.

No trabalho de Eke e Anir (2021) é realizado um mapeamento sistemático (MS), para isso adotou-se a diretriz de revisão de mapeamento sistemático de (PETERSEN *et al.*, 2008) e a diretriz de revisão sistemática da literatura de (KITCHENHAM; BRERETON, 2013), para fornecer uma visão geral do estudo sobre a implementação de mecanismos de solução na mitigação de ameaças e ataques no ambiente BYOD, para isso foram selecionados 69 artigos. A pesquisa revelou que os vazamentos, o roubo de dados e o acesso não autorizados são as ameaças e os ataques BYOD de segurança mais considerados. Já as soluções de controle de acesso, a autenticidade de usuários, a inteligência artificial e o gerenciamento de dispositivos móveis (MDM) foram considerados no domínio. O MS foi realizado para responder a três perguntas de pesquisa em esquemas de classificação que incluem ameaças e ataques, mecanismos de atenuação e facetas de tipo de contribuição.

Os resultados para ameaças e ataques desse MS indicaram que os desafios de *malware*, acesso não autorizado e vazamento e roubo de dados estão recebendo atenção considerável estando presentes em 48% dos estudos primários selecionados. O estudo ainda ressalta como resultado que esses problemas são relativamente dominantes no campo. Em contra partida a rede não confiável, o ataque de *phishing*, as ameaças de violações de dados, a violação de privacidade do usuário, o ataque de espionagem, o ataque de homem do meio, o ataque de falsificação, o ataque de intrusão, a engenharia social, o roubo de privacidade dos dados, a largura de banda, o problema de utilização, a ameaça a persistente avançada e o *botnet* móvel tem menos de 5% cada um dos estudos selecionados, o que revela que menos atenção foi dado a esse domínio.

O estudo também mostrou que, nos mecanismos de atenuação, a solução de controle de acesso, a autenticação do usuário, a técnica de inteligência artificial e o gerenciamento de dispositivos móveis são os mecanismos de solução mais considerados no domínio com 68% dos estudos primários selecionados. Ademais o gerenciamento de aplicativos móveis, o método de detecção de intrusão e a virtualização tem um total de 20% dos estudos selecionado, o que revela um aumento dos mecanismos de solução de segurança no campo. Em contrapartida, mecanismos de solução como detecção de intrusão, gerenciamento de informações móveis, conteinerização, gerenciamento de conteúdo móvel, gerenciamento de mobilidade empresarial, gerenciamento de largura de banda e *blackphone* estão perdendo atenção no domínio.

Na categoria de tipo de distribuição, os resultados da revisão sistemática mostram que os elementos de estrutura, técnica, modelo e sistema receberam a maior atenção, abrangendo 70% dos estudos primários selecionados. Em contrapartida, a abordagem, o protótipo e o método receberam menos destaque no domínio, totalizando menos de 20% dos estudos primários selecionados. Além disso, os resultados também indicam uma tendência de crescimento no nú-

mero de pesquisas nas áreas de estrutura, técnica, modelo e sistema, enquanto os estudos relacionados à abordagem, protótipo e método estão em declínio no domínio.

No trabalho de Coto e Dias (2023), a pesquisa analisou os principais aspectos relacionados a segurança em redes de computadores com ênfase no conceito BYOD, destacando quais as principais vantagens e desvantagens para a segurança da informação das organizações que adotam BYOD. O artigo destaca várias vantagens associadas à implementação de políticas BYOD nas organizações como: aumento da produtividade, redução de custos, flexibilidade e mobilidade e atualização tecnológica. O artigo também menciona desvantagens significativas que podem surgir nas organizações como: riscos a segurança, controle e monitoramento, conformidade e regulamento e privacidade.

Os resultados do estudo indicam que, enquanto o BYOD pode trazer benefícios consideráveis em termos de flexibilidade e redução de custos, é crucial que as organizações implementem políticas de segurança robustas para mitigar os riscos associados. Recomenda-se que as empresas adotem uma abordagem híbrida, combinando medidas de segurança como autenticação multifator, criptografia de dados e soluções de gerenciamento de dispositivos móveis (MDM). Além disso, o artigo sugere que as organizações invistam em treinamento e conscientização dos funcionários sobre práticas seguras de uso de dispositivos, e estabeleçam acordos claros de uso aceitável para equilibrar as vantagens do BYOD com a necessidade de proteger os ativos de informação corporativa.

O trabalho de Boiarski *et al.* (2018), caracterizou o uso de dispositivos móveis pessoais (DMPs) nos Câmpus do Sudoeste do Paraná da UTFPR, afim de fornecer subsídios a construção de uma política institucional de BYOD. A difusão do uso de dispositivos DMPs e a necessidade de conectividade constante nas universidades, como no caso da UTFPR, promovem o uso desses dispositivos para interação e aprendizado. A pesquisa destacou que, à adoção do BYOD oferece benefícios como maior acessibilidade e flexibilidade, mas também exige o desenvolvimento de políticas institucionais para coordenar os recursos necessários, como TI, manutenção e segurança.

A pesquisa utilizou uma abordagem mista, com métodos quantitativos e qualitativos de coleta e análise de dados. A coleta de dados quantitativos foi realizada por meio de um questionário online, respondido por 386 membros da comunidade acadêmica da UTFPR, incluindo alunos, professores e técnicos administrativos. Os dados qualitativos foram coletados por meio de entrevistas semiestruturadas com diretores de ensino, pesquisa, extensão, planejamento e gestão de TI da UTFPR. Os resultados da pesquisa mostraram que o uso de DMP é elevado na UTFPR, com 97,4% dos respondentes relatando o uso de algum tipo de DMP. Os dispositivos mais utilizados são notebooks e smartphones. Os alunos utilizam seus smartphones continuamente ao longo do dia, enquanto os notebooks são utilizados de 3 a 5 vezes por dia. As principais atividades realizadas com os DMP são pesquisas acadêmicas, comunicação e resolução de problemas de trabalho. O estudo destacou que os principais benefícios do uso de DMPs na UTFPR são a utilidade positiva e a eficácia na aprendizagem. Por outro lado, também

apontou as principais limitações, como a infraestrutura insuficiente, as características técnicas dos dispositivos e a falta de capacitação dos usuários.

Além disso, as entrevistas com os diretores da UTFPR confirmaram a necessidade de uma política de gestão de DMPs. Os aspectos mais importantes a serem considerados na elaboração de uma política de BYOD são, a garantia do uso total dos equipamentos, a análise dos investimentos e benefícios, a definição de plataformas, dispositivos controlados e níveis de segurança, e a política de segurança de acesso. Os diretores também destacaram a necessidade de padronização das soluções e serviços de TI em todos os campi da UTFPR. Ademais, o estudo estruturou como contribuição um framework para auxiliar no processo de adoção de uma política de BYOD na UTFPR. O estudo concluiu que a implementação de uma política de BYOD na UTFPR pode trazer benefícios como o aumento da acessibilidade, a promoção da mobilidade e flexibilidade no processo de ensino e aprendizagem, e a melhoria da gestão de recursos de TI. No entanto, também ressalta que, é importante que a política seja elaborada de forma criteriosa, considerando os aspectos técnicos, financeiros e de segurança envolvidos.

Os trabalhos referidos nesta seção destacam a segurança como a principal preocupação associada ao BYOD. Eles analisam o BYOD sob perspectivas complementares, proporcionando uma visão abrangente dos desafios e benefícios dessa prática no ambiente corporativo. Em comum, os estudos reconhecem a importância de uma abordagem robusta e multifacetada para mitigar os riscos de segurança associados ao BYOD. A partir das informações obtidas pode-se concluir que, apesar dos benefícios evidentes do BYOD, como aumento da produtividade e redução dos custos, as organizações precisam implementar políticas de segurança eficazes e integradas que abranjam controles tecnológicos, gerenciais e comportamentais como: o desenvolvimento e implementação de políticas de segurança claras e abrangentes que cubram todos os aspectos do BYOD; a utilização de soluções tecnológicas avançadas, como controle de acesso, MDM, e inteligência artificial para detectar e responder ameaças; e investimento em treinamento contínuo através de programas de educação e conscientização para garantir que os funcionários compreendam e sigam as práticas de segurança. Destacando assim, a importância de uma estratégia equilibrada que maximize os benefícios do BYOD enquanto minimiza os riscos associados à segurança da informação. Essa abordagem holística é fundamental para proteger os ativos de informação das organizações e garantir a conformidade com as normas de segurança da informação, permitindo que as organizações aproveitem os benefícios do BYOD sem comprometer a segurança.

4 MATERIAIS E MÉTODOS

Este capítulo descreve os procedimentos metodológicos adotados para atingir os objetivos propostos neste trabalho de conclusão de curso.

4.1 Materiais

Este estudo baseia-se em uma abordagem teórica, fundamentada principalmente em materiais acadêmicos, artigos científicos, livros e normas técnicas. Esses recursos proporcionam uma visão atualizada sobre o tema. A abordagem adotada fundamentou-se em referências teóricas extraídas de artigos científicos, livros especializados, normas técnicas e publicações institucionais, além da realização de um estudo de caso aplicado.

A construção da base teórica da pesquisa foi pautada, principalmente em artigos publicados em periódicos, com destaque para aqueles indexados na plataforma IEEE[1]. Essa escolha justifica-se pela credibilidade da plataforma e devido à atualização constante dos estudos disponíveis, os quais oferecem uma visão aprofundada sobre o tema abordado. A seleção dos artigos foi facilitada pela ferramenta Google Acadêmico[2], que possibilitou o acesso a uma variedade ainda maior de publicações científicas provenientes de diferentes bases de dados. Os critérios da busca baseou-se na relevância para o tema e atualidade dos estudos.

Além dos artigos acadêmicos, a pesquisa também se apoiou em normas e publicações técnicas voltadas à área de Segurança da Informação. Esses documentos foram essenciais para definição de parâmetros metodológicas e diretrizes alinhadas às melhores práticas internacionais, sendo consultados principalmente por meio de plataformas institucionais e bases de pesquisa acadêmica. Outro pilar fundamental da pesquisa, foi a consulta de livros e capítulos de livros especializados, que forneceram um embasamento teórico sólido, tanto do ponto de vista conceitual quanto histórico sobre os conceitos e práticas abordados nesta pesquisa.

Por fim, além da pesquisa bibliográfica, o estudo incluiu um estudo de caso realizado na Coordenadoria de Gestão de Tecnologia da Informação da Universidade Tecnológica Federal do Paraná, Campus Toledo (COGETI-TD). Essa abordagem permitiu a verificação dos conceitos teóricos discutidos, proporcionando uma compreensão mais detalhada e contextualizada do tema investigado.

4.2 Métodos

O presente trabalho adotou uma abordagem baseada em pesquisa bibliográfica e estudo de caso. Inicialmente, foi realizada uma revisão bibliográfica com o objetivo de aprofundar o embasamento teórico sobre a prática de BYOD, políticas e normas de segurança da informação,

[1] Disponível em: https://ieeexplore.ieee.org/

[2] Disponível em: https://scholar.google.com.br/

além de estratégias para mitigação de riscos em ambientes que adotam essa prática. Para isso, foram analisadas instruções normativas de segurança, políticas de BYOD de organizações, artigos acadêmicos e livros especializados.

Em seguida, foi conduzido um estudo de caso na COGETI-TD, por meio de entrevistas com os servidores Leandro Carvalho, Matheus Bessegato e Jorge Otta. O estudo permitiu constatar que, embora a instituição não possua uma política formal de BYOD, essa prática está presente e conta com a aplicação de medidas de segurança. Entre os controles adotados, destacam-se o princípio do privilégio mínimo, a segmentação de redes por VLANs e a autenticação de usuários na rede Wi-Fi.

Por fim, a pesquisa possibilitou a identificação das principais estratégias de mitigação de riscos, bem como os benefícios e desafios do BYOD. Com base nesses achados, foram elaboradas recomendações de melhores práticas para aprimorar a segurança na adoção do BYOD, fornecendo subsídios para profissionais e organizações que buscam implementar ou fortalecer essa prática.

5 ESTUDO DE CASO

Um estudo de caso é uma metodologia de pesquisa utilizada para explorar e analisar um fenômeno específico dentro de seu contexto real, proporcionando uma compreensão de como e por que certos eventos ocorrem. Neste sentido, um estudo de caso foi conduzido na Universidade Tecnológica Federal do Paraná, Campus Toledo (UTFPR-TD), com o objetivo de identificar se a instituição, que comporta um grande número de dispositivos eletrônicos e provê acesso à Internet e a alguns serviços locais, possui diretrizes específicas sobre a política de *Bring Your Own Device*. A UTFPR-TD enfrenta desafios relacionados à gestão da utilização de dispositivos pessoais de usuários, compostos por alunos, professores e servidores, especialmente no que diz respeito à segurança, eficiência operacional e experiência dos usuários. Este estudo busca compreender a relação entre a utilização de dispositivos pessoais em uma organização ao qual a prática de BYOD pode ser benéfica.

A implementação de BYOD em instituições de ensino superior pode trazer benefícios significativos, como a flexibilidade e a personalização dos recursos tecnológicos pelos usuários. No entanto, também pode apresentar desafios consideráveis, especialmente relacionados à segurança da informação, gestão de dispositivos e a manutenção. O objetivo deste estudo é identificar e avaliar a existência de diretrizes específicas sobre BYOD na UTFPR-TD, bem como analisar os impactos desta prática na segurança, eficiência operacional e experiência dos usuários.

A metodologia deste estudo de caso baseia-se em uma visita realizada no dia 3 de junho de 2024 à Coordenadoria de Gestão de Tecnologia da Informação da Universidade Tecnológica Federal do Paraná, Campus Toledo (COGETI-TD). Durante a visita, foram conduzidas entrevistas com os servidores Leandro Carvalho, Matheus Bessegato e Jorge Otta, que responderam a uma série de questões relacionadas à política de *Bring Your Own Device* e à segurança da informação na instituição. A entrevista foi realizada com o objetivo de obter informações sobre a existência e a implementação de diretrizes específicas sobre BYOD, os desafios enfrentados pela universidade em relação à gestão de dispositivos pessoais e as medidas de segurança adotadas. Os dados coletados a partir dessa entrevista formam a base da análise deste estudo e são apresentadas a seguir.

Em um primeiro momento, nota-se que a instituição não possui uma política formal de BYOD. Entretanto, a COGETI-TD aplica controles de segurança adequados para que tanto computadores fornecidos pela instituição quanto computadores e dispositivos móveis pessoais de usuários sejam utilizados dentro do campus, fazendo uso da rede de comunicação da instituição para acessar a Internet. Em resumo, embora não haja uma formalidade, aplica-se a prática de BYOD. A seguir, é melhor descrito como isto ocorre.

A instituição disponibiliza computadores, como *desktops* e *notebooks*, para servidores e docentes. Todavia, esses equipamentos nem sempre são novos ou adequados para executar todas as tarefas da maneira desejada pelos usuários. Todos os dispositivos disponibilizados aos

usuários pela instituição são preparados pela COGETI-TD, que os configura para uso adequado. Contudo, a quantidade de equipamentos não é suficiente para atender a todo o quadro de servidores e docentes, sendo uma demanda constante. Este é um dos fatores que motivam os usuários a optarem por utilizar dispositivos próprios enquanto estão na instituição. Portanto, é necessário compreender como isso se torna possível e quais são os controles empregados para garantir a segurança.

Inicialmente, é identificado que não há diferenciação no tratamento do tráfego entre dispositivos pertencentes à instituição e aqueles de propriedade dos usuários. No entanto, a diferenciação do tráfego ocorre com base no princípio de segregação de funções, focando no tipo de usuário, e não no dispositivo utilizado. O princípio de segregação de funções é uma prática na qual o controle de acesso e permissões é baseado no tipo de usuário e nas suas responsabilidades dentro da organização. Esse princípio estabelece que diferentes funções e responsabilidades devem ser atribuídas a diferentes indivíduos dentro de um sistema ou processo, de modo que uma pessoa não tenha controle absoluto sobre uma operação crítica. Isso ajuda a mitigar riscos ao limitar o potencial de erros acidentais ou intencionais e reduzir o impacto de uma possível violação de segurança. Na prática, o usuário é conectado a uma VLAN (*Virtual Local Area Network*) de acordo com as credenciais apresentadas para inserção na rede. Uma VLAN é uma tecnologia de rede que permite segmentar uma rede física em múltiplas redes lógicas independentes. Utilizando VLANs, dispositivos conectados ao mesmo *switch* físico podem ser agrupados em diferentes domínios de *broadcast*, melhorando a segurança, a eficiência do tráfego de rede e a gestão administrativa. Cada VLAN funciona como uma rede separada, isolando o tráfego e permitindo políticas de acesso específicas, facilitando o controle de acesso e a segregação de funções dentro de uma organização. No âmbito da UTFPR-TD, isto implica, por exemplo, que o dispositivo de um usuário classificado como “aluno” não “enxergará” uma estação de impressão, que deve ser disponibilizada apenas à docentes e servidores da instituição. Isto é, os dispositivos dos alunos e a estação de impressão não encontram-se no mesmo segmento lógico da rede.

A disponibilização de computadores para docentes ou servidores inclui a implementação de medidas de segurança para proteger os dados e sistemas da instituição. Entre essas medidas, destaca-se a utilização do princípio de privilégio mínimo. O princípio de privilégio mínimo, ou *least privilege principle* (JERO *et al.*, 2021), é um conceito fundamental em segurança da informação e gestão de acesso. Ele estipula que qualquer entidade (usuário, processo, sistema) deve ter apenas as permissões necessárias para realizar suas funções específicas e nada mais. Em outras palavras, cada entidade deve operar com o menor nível de privilégio que permita a execução das suas tarefas autorizadas, sem acesso adicional que possa ser potencialmente explorado por atacantes. Isso ajuda a minimizar o risco de comprometimento do sistema, limitando o impacto de eventuais violações de segurança. O princípio de privilégio mínimo é normalmente adotado em ambientes de TI para garantir um controle sobre os acessos e reduzir a superfície de ataque disponível para potenciais ameaças.

Na prática, o computador oferecido ao docente ou servidor, é entregue pela COGETI-TD com antivírus e um conjunto de *softwares* básicos, considerados essenciais para o desempenho das funções acadêmicas e administrativas. Instalar apenas o mínimo de *softwares* necessário é mais seguro porque reduz a superfície de ataque disponível para potenciais ameaças. Cada software instalado representa uma possível vulnerabilidade que pode ser explorada por crackers. Além disso, limitar o número de *softwares* simplifica a gestão de segurança, permitindo uma melhor focalização na monitorização e proteção dos aplicativos essenciais. Menos *softwares* instalados significam menos complexidade, menor probabilidade de conflitos entre programas e uma redução geral nos riscos associados a *softwares* maliciosos ou erros de configuração. Isso resulta não só em um ambiente mais seguro, mas também em um sistema mais estável e eficiente. Além disso, sempre que um usuário deseja instalar um *software* adicional, é necessário que ele faça uma solicitação formal por meio da abertura de um chamado. A COGETI-TD avalia e aprova essa solicitação antes de proceder com a instalação, garantindo que apenas *softwares* autorizados e licenciados sejam adicionados ao sistema, evitando assim a utilização de *softwares* inseguros ou de versões que possam trazer consigo algum tipo de *malware*.

Entretanto, o princípio de privilégio mínimo não é aplicado em sua totalidade para usuários mais experientes, como por exemplo, para docentes dos cursos de computação. Esses usuários, devido ao seu maior nível de experiência e às suas necessidades específicas, muitas vezes requerem acesso a funções administrativas e outras operações avançadas que exigem permissões mais amplas. Dessa forma, é permitido que esses usuários tenham um nível de acesso mais elevado, ajustando-se às suas necessidades acadêmicas e operacionais, enquanto ainda se busca manter um ambiente seguro e controlado.

Quando o usuário opta por utilizar seu próprio dispositivo para desenvolver suas atividades na instituição, não há restrições de acesso, tampouco exigências adicionais para garantir a segurança. As diretrizes aplicáveis aos dispositivos pessoais são equivalentes às aplicadas aos dispositivos institucionais, visto que as medidas de segurança estão associadas ao nível de permissão de cada usuário, e não aos dispositivos em si. O *firewall*, que é um dispositivo de segurança de rede que monitora e controla o tráfego de entrada e saída com base em regras de segurança predefinidas, não diferencia os dispositivos, ou seja, o tráfego é tratado de forma idêntica para dispositivos institucionais e pessoais.

O acesso principal à internet da instituição é fornecido pela Rede Nacional de Ensino e Pesquisa (RNP), que serve como provedor de Internet para diversas instituições educacionais no Brasil. Dentro da estrutura da RNP, o Centro de Atendimento a Incidentes de Segurança (CAIS) adiciona uma camada extra de segurança. Especializado em segurança da informação, o CAIS tem como objetivo fortalecer a proteção das redes acadêmicas e de pesquisa conectadas à RNP. Além de oferecer suporte técnico especializado, o CAIS realiza monitoramento contínuo e coordenação na resposta a incidentes de segurança cibernética, utilizando ferramentas avançadas e técnicas especializadas para identificar e analisar ameaças em tempo real. O CAIS

é responsável por emitir boletins periódicos com recomendações e também alertas de novas vulnerabilidades descobertas. Isto é importante, pois, permite aos servidores da COGETI-TD manterem-se atualizados e prontos para evitarem ataques que baseiam-se em explorar novas vulnerabilidades.

Além das atividades de conscientização e informação, o CAIS atua proativamente na detecção de problemas. Por exemplo, foram registrados incidentes relacionados ao uso de dispositivos pessoais no campus, como a instalação de *softwares* piratas em dispositivos que acessam a Internet pela rede da instituição. A análise revelou comunicações desses dispositivos com servidores desconhecidos, muitas vezes facilitadas por *cracks*. Ao identificar a origem do tráfego suspeito, a RNP intervém para identificar e interromper essa atividade. Nos casos envolvendo computadores institucionais, o software ilegal é imediatamente removido. Para dispositivos pessoais, os usuários são orientados a desinstalar o *software* pirata.

Uma característica significativa que demonstra o incentivo da instituição ao uso de dispositivos móveis pessoais é a cobertura WiFi em quase todo o campus. O acesso à rede é restrito a usuários credenciados, que devem autenticar com suas credenciais no momento de conexão. Além disso, a maioria dos *access points* (AP), dispositivos que facilitam a conexão de dispositivos sem fio à rede cabeada, suporta gerenciamento centralizado e implementação de controles de segurança. Por exemplo, esses dispositivos têm a capacidade de detectar um tipo de ataque conhecido como Rogue AP. Um Rogue AP ocorre quando um *access points* não autorizado é implantado em uma rede sem fio sem o consentimento dos administradores, podendo ser malicioso, quando usado para enganar usuários e interceptar dados sensíveis, ou não intencional, quando um dispositivo legítimo mal configurado se comporta como um rogue AP devido a falhas de segurança ou configuração inadequada. Quando um Rogue AP é detectado, os *access points* da instituição podem alternar temporariamente para um modo cliente, efetivamente realizando um ataque de negação de serviço (Denial of Service - DoS) contra o Rogue AP para impedir que usuários se conectem a ele.

Um dos desafios enfrentados pela instituição é o *phishing*, uma prática comum de ciberataque que visa obter informações privadas, seja de organizações ou usuários individuais. De acordo com (CERT.br, 2012), “o *phishing* é o tipo de fraude por meio do qual um golpista tenta obter dados pessoais e financeiros de um usuário, pela utilização combinada de meios técnicos e engenharia social”. Na prática, esses ataques consistem na tentativa de obter informações confidenciais, como senhas, números de cartões de crédito ou outras credenciais, de maneira ilícita.

Na instituição, alertas já foram enviados a servidores e estudantes sobre tentativas de golpes envolvendo *phishing*, nas quais os atacantes se passavam por setores institucionais para induzir as vítimas a clicar em *links* maliciosos ou compartilhar dados sigilosos. Comumente realizados por *e-mail*, os ataques de *phishing* frequentemente envolvem criminosos que simulam ser entidades confiáveis, como bancos, empresas ou mesmo instituições de ensino, para enganar as vítimas. Cada vez mais sofisticados, esses ataques representam ameaças significativas,

podendo levar ao roubo de identidade, perdas financeiras, danos à reputação das instituições e disseminação de *malware*. A eficácia do *phishing* está na exploração da confiança do usuário e na habilidade dos atacantes em criar um senso de urgência ou curiosidade, incentivando a interação com o conteúdo malicioso. Ainda de acordo com o (CERT.br, 2012), o *phishing* é caracterizado por meio do envio de mensagens eletrônicas que:

- Tentam se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um site popular;
- Procuram atrair a atenção do usuário, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira;
- Informam que a não execução dos procedimentos descritos pode acarretar sérias consequências, como a inscrição em serviço de proteção de crédito e o cancelamento de um cadastro, de uma conta bancária ou de um cartão de crédito;
- Tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas, que tentam se passar pela página oficial da instituição; da instalação de códigos maliciosos, projetados para coletar informações sensíveis; e do preenchimento de formulários contidos na mensagem ou em páginas Web.

De acordo com a (IBM, 2023), o *phishing* caracteriza-se como uma técnica sofisticada de engenharia social. Os ataques de engenharia social manipulam as pessoas para compartilhar informações que não deveriam compartilhar, baixar *software* que não deveriam baixar, visitar sites que não deveriam visitar, enviar dinheiro para criminosos ou cometer outros erros que comprometam sua segurança pessoal ou organizacional. Nesse sentido a engenharia social utiliza-se de táticas de manipulação psicológica e explora o erro ou a falta de conhecimento humano em vez de vulnerabilidades técnicas. Manipulando as vítimas, para conseguir informações sigilosas com a finalidade de realizar um ataque que pode comprometer a segurança pessoal ou a segurança de uma rede corporativa. Isso torna evidente que ausência de uma estratégia de educação voltada para os usuários é um fator determinante que contribui para a vulnerabilidade da instituição diante de ataques de *phishing*.

O estudo de caso realizado na UTFPR-TD possibilitou compreender, na prática, a dinâmica de uma organização ao lidar com a gestão de dispositivos, tanto institucionais quanto pessoais, identificando os perigos e riscos associados. Constatou-se que, apesar da ausência de uma política formal de BYOD, a instituição adota práticas que possibilitam o uso de dispositivos móveis pessoais de forma integrada às suas operações, permitindo que a adesão da prática de BYOD seja funcional e segura. De modo que, a inexistência de uma politica estruturada de BYOD não impediu a adoção de práticas voltadas para garantir a segurança da informação como a implementação de controles de segurança, tais como o princípio do privilégio mínimo, a segmentação de rede por VLANs e autenticação de usuários na rede WiFi. Essas abordagens,

demonstram o esforço da instituição para conciliar a flexibilidade proporcionada pelo BYOD com necessidade de proteção dos dados institucionais, da rede, bem como a eficiência operacional, mesmo em um ambiente de alta heterogeneidade de dispositivos.

Observou-se que a infraestrutura tecnológica da universidade como a cobertura abrangente de WiFi e a gestão centralizada dos *access points*, contribui para a experiência positiva dos usuários e para mitigação de riscos de segurança, como ataques de Rogue AP. Em contrapartida, os desafios identificados, como a presença de *softwares* não autorizados em dispositivos pessoais e ataques de *phishing* persistem e requerem esforços contínuos de conscientização e intervenção técnica. De modo que, ressaltam a complexidade de adotar práticas de BYOD em um ambiente acadêmico diverso. Adicionalmente, verificou-se que o suporte oferecido pela RNP e o CAIS fortalece a infraestrutura de segurança da instituição, garantido monitoramento continuo e ações preventivas contra vulnerabilidades. Ressaltando o comprometimento da UTFPR-TD com a segurança cibernética.

Por fim, conclui-se que, embora a prática de BYOD traga benefícios como flexibilidade e personalização, sua adoção requer a implementação de diretrizes mais robustas e formalizadas. Isso permitirá a instituição alinhar-se as melhores práticas de governança de TI, aprimorando a eficiência operacional, a segurança da informação e a experiência dos usuários, sem comprometer os objetivos acadêmicos e administrativos da instituição.

6 RECOMENDAÇÕES

Este capítulo apresenta um conjunto de recomendações para organizações que desejam implementar a prática de BYOD de forma segura e eficiente. Além disso, são apresentadas as principais técnicas empregadas para mitigar os riscos inerentes a essa abordagem, buscando equilibrar a flexibilidade proporcionada pelo uso de dispositivos pessoais com a necessidade de proteção das informações institucionais. As diretrizes e técnicas apresentadas têm como objetivo auxiliar as organizações na adoção de práticas que promovam a segurança, a integridade dos dados e a eficiência operacional em um cenário de alta diversidade tecnológica.

6.1 Recomendações para Organizações que Adotam BYOD

Com base na literatura sobre o tema, as recomendações mais frequentemente direcionadas às organizações que optam por adotar a prática de BYOD incluem:

- **Desenvolver uma Política Formal de BYOD**.

A implementação de uma Política Formal de BYOD deve abranger diversos aspectos, com o objetivo de garantir a segurança da informação, a proteção de dados corporativos e a definição clara de responsabilidades entre a organização e seus colaboradores. Primeiramente, no que se refere ao uso permitido, a política deve especificar quais aplicativos e sistemas corporativos podem ser acessados pelos dispositivos pessoais, incluindo e-mails corporativos, intranet, sistemas de gestão e aplicativos específicos da empresa. Além disso, é imprescindível que sejam estabelecidos os tipos de dados que podem ser manipulados, com a devida diferenciação entre dados confidenciais, sensíveis e públicos, para assegurar que informações críticas sejam tratadas de maneira adequada. A localização do acesso aos sistemas corporativos também precisa ser definida, restringindo-o a áreas específicas, como dentro das instalações da empresa ou por meio de redes Wi-Fi seguras e VPN. Também é importante estabelecer horários específicos para o acesso aos sistemas, com atenção especial aos dados confidenciais. No que tange às restrições de uso, deve-se proibir *downloads* não autorizados, acesso a sites não relacionados ao trabalho ou o compartilhamento de informações confidenciais com terceiros. Ademais, a política deve especificar as responsabilidades dos colaboradores quanto à proteção de dados corporativos e instituir sanções claras para o não cumprimento das diretrizes.

No que se refere à segurança da informação, a política deve exigir o registro e a manutenção de um inventário atualizado de todos os dispositivos autorizados, incluindo informações como modelo, sistema operacional e aplicativos instalados. A utilização de senhas fortes e a implementação de autenticação multifatorial (MFA) são medidas cruciais, assim como a configuração de bloqueio automático dos dispositivos após um período de inatividade. No que diz respeito à criptografia de dados, é imperativo que todos os dados sensíveis armazenados nos dispositivos sejam criptografados para evitar acessos não autorizados, em casos de perda ou

roubo de dispositivos. Além disso, durante a transmissão de dados, deve-se utilizar protocolos seguros, como HTTPS, para proteger os dados em trânsito. Em relação às atualizações de *software*, a política deve exigir que os dispositivos estejam sempre atualizados com as versões mais recentes do sistema operacional e dos aplicativos, além de implementar um sistema de gerenciamento de *patches* para garantir a aplicação rápida de correções de segurança. O gerenciamento de dispositivos móveis (MDM) deve ser implementado para monitorar e proteger os dispositivos remotamente, permitindo funcionalidades como bloqueio remoto, apagamento de dados e localização do dispositivo, especialmente em caso de perda ou roubo. Além disso, é necessário garantir o uso de redes Wi-Fi seguras e criptografadas, além de recomendar o uso de VPN para o acesso remoto aos sistemas corporativos. Procedimentos claros devem ser estabelecidos para casos de perda ou roubo de dispositivos, e a conscientização dos colaboradores sobre boas práticas de segurança deve ser reforçada por meio de treinamentos regulares. Por fim, Auditorias periódicas devem ser realizadas para garantir a conformidade com a política de BYOD e investigar e documentar todos os incidentes de segurança relacionados a dispositivos pessoais, a fim de revisar continuamente as práticas de segurança e garantir a proteção dos dados corporativos.

No que tange às responsabilidades do usuário, a política deve deixar claro que o colaborador é responsável pela segurança do dispositivo pessoal e pelos dados corporativos nele armazenados, além de especificar as obrigações de proteção de dados e as sanções em caso de violação. O colaborador também deve ser responsabilizado pela proteção física do dispositivo, a fim de evitar roubo, perda ou danos. Em caso de incidentes de segurança, como perda do dispositivo ou suspeitas de acesso não autorizado, o colaborador deve notificar imediatamente a equipe de TI, permitindo a adoção de medidas de proteção, como o bloqueio remoto do dispositivo. A política deve esclarecer que os dados corporativos armazenados no dispositivo são de propriedade da organização e devem ser excluídos de forma segura em casos de desligamento do colaborador ou perda do dispositivo.

No que se refere ao suporte técnico, a política deve especificar os tipos de suporte oferecidos pela organização para os dispositivos pessoais, como a configuração inicial, a instalação de aplicativos corporativos e a resolução de problemas relacionados à conexão com a rede corporativa. Deve ser claramente estabelecido que a organização não será responsável por reparos de *hardware*, recuperação de dados pessoais ou manutenção geral do dispositivo, com o suporte técnico limitado ao uso corporativo. Além disso, para que o colaborador receba suporte, ele deve autorizar o acesso remoto ou físico ao dispositivo, garantindo que a privacidade dos dados pessoais seja respeitada e que a autorização seja registrada de forma adequada, a fim de garantir transparência e conformidade com as políticas de segurança.

A definição de tipos de dispositivos permitidos e configurações mínimas de segurança é fundamental para garantir a integridade dos sistemas em ambientes que adotam a prática de BYOD. A política de segurança deve especificar os tipos de dispositivos autorizados, como

smartphones, *tablets* e *notebooks*, levando em consideração a compatibilidade com os sistemas corporativos. Além disso, a empresa pode estabelecer uma lista de marcas e modelos de dispositivos permitidos, com o objetivo de garantir maior controle sobre a infraestrutura de TI e sua segurança. A política também deve definir os sistemas operacionais compatíveis, restringindo o acesso a aqueles que não são suportados ou desconhecidos pela organização, além de exigir que esses sistemas operacionais sejam regularmente atualizados para mitigar vulnerabilidades. A definição de requisitos mínimos de *hardware* e *software*, como capacidade de armazenamento, processamento e memória RAM, também é necessária para garantir o desempenho adequado das aplicações corporativas.

No tocante às configurações de segurança, é essencial que os dispositivos estejam sempre atualizados com as versões mais recentes do sistema operacional e dos aplicativos, a fim de corrigir vulnerabilidades e fortalecer a proteção contra ameaças. A instalação de *softwares* de segurança, como antivírus e *firewalls*, deve ser obrigatória, a fim de proteger os dispositivos contra ataques cibernéticos. A política deve, ainda, proibir a modificação dos dispositivos, como o *jailbreak* ou *root*, que comprometem a segurança do sistema e permitem a instalação de aplicativos não autorizados. A criptografia de dados em repouso e em trânsito é altamente recomendada, especialmente para proteger informações confidenciais em dispositivos que possam ser perdidos ou roubados.

- **Educação e Conscientização dos Usuários**.

A educação e a conscientização dos usuários configuram-se como pilares fundamentais para o fortalecimento da segurança em uma política de BYOD. A implementação de treinamentos regulares que abordam boas práticas de segurança cibernética, estratégias para identificar e prevenir ataques de *phishing* e a conscientização sobre os perigos inerentes à instalação de *softwares* não autorizados constitui uma abordagem necessária. Paralelamente, a promoção de campanhas contínuas de sensibilização é essencial para fortalecer a compreensão dos colaboradores sobre os riscos associados ao BYOD, destacando sua responsabilidade direta na proteção dos dados organizacionais. Essas iniciativas não apenas elevam o nível de conscientização dos usuários, mas também criam uma cultura organizacional voltada à segurança, reduzindo a vulnerabilidade a incidentes e garantindo a conformidade com a política.

- **Segmentação da Rede**.

A segmentação da rede em políticas de BYOD é uma prática essencial para mitigar riscos de segurança e garantir o controle adequado do tráfego de dados entre dispositivos pessoais e a rede corporativa. A implementação de uma segmentação de rede robusta, envolve a criação de redes separadas para dispositivos pessoais e corporativos, permitindo que cada dispositivo tenha acesso limitado e controlado aos recursos da organização. A segmentação pode ser realizada através de VLANs específicas para dispositivos pessoais, que limitam o cesso a rede corporativa principal que contém recursos e informações sensíveis, evitando a propaga-

ção de ameaças e restringindo o acesso dos dispositivos pessoais a recursos criticos e dados confidenciais do sistema corporativo.

- **Implementar o Princípio do Privilégio Mínimo**.

Em uma política de BYOD, a adoção do princípio do privilégio mínimo é fundamental para garantir que cada dispositivo pessoal utilizado pelos colaboradores tenha acesso limitado às informações e sistemas indispensáveis para a execução de suas funções profissionais. Além disso, é necessário realizar revisões periódicas dos privilégios de acesso, com o objetivo de garantir seu atendimento às necessidades reais do colaborador, minimizando riscos de exposição indevida de dados e promovendo a segurança da informação de forma contínua.

- **Políticas de Gerenciamento de Aplicativos**.

No contexto do gerenciamento de aplicativos em uma política de BYOD, é essencial estabelecer uma lista de aplicativos corporativos previamente planejados, restringindo o uso de aplicativos não autorizados ou considerados potencialmente inseguros. Além disso, é fundamental promover a adoção de soluções corporativas específicas para atividades determinadas, garantindo a proteção dos dados organizacionais e a eficiência operacional. A implementação de soluções de Gerenciamento de Dispositivos Móveis (MDM) ou Gerenciamento de Aplicativos Móveis (MAM) é altamente recomendada, pois possibilita um controle centralizado e eficiente sobre os aplicativos utilizados, contribuindo para a mitigação de riscos e para a conformidade com as políticas de segurança da organização.

As políticas podem ainda, instituir a introdução do Gerenciamento Unificado de *Endpoints* (UEM), que implementa uma abordagem ainda mais abrangente e eficiente para o gerenciamento de dispositivos e aplicativos. Uma vez que UEM combina funcionalidades do MDM e do MAM com ferramentas avançadas de gerenciamento de PCs e dispositivos locais, permitindo uma administração centralizada que abrange dispositivos móveis, *desktops* e até mesmo dispositivos de IoT.

- **Monitoramento e Auditoria Contínuos**.

No contexto da implementação de uma política de BYOD, deve-se instituir o monitoramento contínuo e a realização de auditorias regulares dos dispositivos conectados à rede como práticas indispensáveis para a identificação de atividades suspeitas e para garantir a aderência às políticas de segurança condicional da organização. A utilização de ferramentas avançadas de monitoramento de tráfego de rede, aliadas a auditorias sistemáticas, possibilita a detecção precoce de vulnerabilidades, bem como a implementação de medidas proativas para a mitigação de riscos. Essas práticas não apenas fortalecem a proteção dos dados corporativos, mas também promovem a conformidade regulatória e a integridade das informações confidenciais.

- **Plano de Resposta a Incidentes**.

No contexto de uma política de BYOD, é necessário que a organização implemente um plano de resposta a incidentes de segurança devidamente estruturados e alinhados às melhores práticas do setor. Esse plano deve incluir etapas claras e definidas para a identificação, contenção, análise, recuperação e comunicação de incidentes, garantindo uma abordagem sistemática e eficiente na mitigação de riscos. A comunicação ágil com as partes envolvidas, incluindo equipes de TI, gestores e colaboradores, é fundamental para garantir uma resposta coordenada, enquanto a rápida recuperação de dados críticos desempenha um papel essencial na manutenção da continuidade operacional. Além disso, a documentação e o aprendizado obtidos com cada incidente devem ser incorporados à política de segurança, promovendo melhorias contínuas no processo de gestão de riscos e reforçando a resiliência organizacional frente às ameaças inerentes ao uso de dispositivos pessoais.

De modo resumido, a Tabela 1 sintetiza as recomendações, dividindo-as em categorias principais e destacando os pontos mais relevantes.

Categoria	Recomendação	Principais Aspectos
Política Formal de BYOD	Desenvolver uma política formal	Uso permitido, segurança da informação, responsabilidades, suporte técnico, dispositivos permitidos.
Educação e Conscientização	Realizar treinamentos e campanhas contínuas	Identificação de ataques, boas práticas, responsabilidade direta na proteção dos dados organizacionais.
Segmentação de Rede	Criar redes separadas para dispositivos pessoais	Implementação de VLANs para limitar acesso a recursos sensíveis e proteger dados corporativos.
Princípio do Privilégio Mínimo	Limitar acesso a informações indispensáveis	Revisão periódica de privilégios, minimizando riscos de exposição indevida.
Gerenciamento de Aplicativos	Listar e restringir aplicativos permitidos	Adoção de MDM/MAM, UEM, e soluções corporativas específicas.
Monitoramento e Auditoria	Implementar ferramentas avançadas de monitoramento e auditoria contínua	Identificação de atividades suspeitas e garantia da conformidade com as políticas de segurança.
Plano de Respostas a Incidentes	Implementar um plano estruturado de resposta a incidentes	Definir etapas claras para identificação, contenção, análise, recuperação e comunicação de incidentes

Tabela 1 – Recomendações para implementação de BYOD

6.2 Técnicas Utilizadas para Mitigação de Riscos no BYOD

Com base na literatura especializada, as técnicas mais frequentemente empregadas para mitigar os riscos associados à adoção do BYOD incluem:

- **Segregação de Dados e Aplicativos**.

1. Uso de containers ou *sandboxes* para isolar dados corporativos dos pessoais no dispositivo.

A segregação de dados e aplicativos é uma estratégia essencial para isolar as informações corporativas das pessoais em dispositivos de propriedade do usuário no contexto BYOD. O uso de contêineres ou *sandboxes* permite a criação de ambientes isolados dentro do dispositivo, nos quais os dados e aplicativos corporativos podem ser armazenados e operados separadamente dos dados pessoais. Essa abordagem visa proteger a confidencialidade das informações empresariais, evitando o acesso não autorizado ou a troca inadvertida de dados entre os ambientes corporativo e pessoal.

Os contêineres são uma forma de virtualização em nível de sistema operacional. Eles permitem a execução de um aplicativo e suas dependências de forma isolada, mas de maneira mais leve e eficiente em comparação com a virtualização tradicional. No caso dos contêineres, o sistema operacional principal funciona como um hospedeiro e compartilha o *kernel*, mas cada contêiner tem seu próprio espaço de usuário e sistema de arquivos. A tecnologia mais conhecida de contêineres é o Docker. Os contêineres são populares no desenvolvimento e na execução de microsserviços. Os *sandboxes* são ambientes isolados criados para testar e executar código de maneira segura, sem afetar o sistema operacional principal. A principal função de uma *sandbox* é proteger o sistema de potencial código malicioso ou *bugs*, já que qualquer falha ou comportamento inesperado do código dentro da *sandbox* não afetará o restante do sistema. As *sandboxes* são usadas, por exemplo, para testar novos *softwares* ou para rodar aplicativos de forma controlada. Ambos os conceitos visam segurança, controle de recursos e eficiência na execução de tarefas, mas diferem em como eles são implementados e no nível de isolamento que oferecem.

2. Garantir que aplicativos corporativos funcionem de forma independente dos pessoais.

Além disso, a garantia de que os aplicativos corporativos funcionem de maneira independente dos aplicativos pessoais é fundamental para mitigar o risco de vazamento de dados ou de interferências indesejadas. A segregação pode ser realizada por meio de tecnologias como containers, virtualização ou abordagens fundamentadas em politicas de segurança que definem claramente as fronteiras entre os dados corporativos e pessoais, impondo restrições rígidas ao compartilhamento e ao acesso entre os dois ambientes.

- **Autenticação e Controle de Acesso**.

1. Implementação de autenticação multifator (MFA) para acesso a sistemas e redes.

A implementação de autenticação multifatorial (MFA) é uma das estratégias mais eficazes para mitigar os riscos relacionados ao acesso a sistemas e redes corporativas por dispositivos pessoais. A MFA é um processo de autenticação que requer que os usuários forneçam múltiplos fatores de verificação (tais como senhas, biometria ou *tokens*) antes de conceder acesso a sistemas e redes, o que aumenta significativamente a segurança, dificultando o acesso não autorizado, mesmo que credenciais como senhas sejam comprometidas.

A técnica combina diferentes tipos de fatores de autenticação, que são classificados em três categorias principais:

- Fatores de Conhecimento: que são informações que o usuário conhece como senhas, PINs ou respostas a perguntas de segurança;
- Fatores de Posse: que são elementos físicos que o usuário possui, como cartões inteligentes, *tokens* de *hardware* ou dispositivos móveis com aplicativos autenticadores. Esses dispositivos geram códigos temporários ou fornecem formas de autenticação baseada em criptografia, o que torna a autenticação mais robusta; e
- Fatores Inerentes: esses fatores referem-se a características físicas únicas do usuário, como impressões digitais, padrões faciais, voz ou íris. A biometria, tem sido progressivamente incorporada a sistemas de autenticação, é um dos fatores mais difíceis de replicar ou transferir.

A MFA não apenas dificulta o acesso não autorizado, mas também oferece uma resposta eficaz contra os riscos de segurança associados ao uso de dispositivos pessoais no ambiente de trabalho.

2. Uso de certificados digitais para autenticação de dispositivos.

A utilização de certificados digitais para autenticação de dispositivos constitui uma técnica adicional relevante, pois esses certificados são empregados para validar a identidade de dispositivos e assegurar que somente dispositivos previamente autorizados possam acessar recursos corporativos. A implementação de autenticação baseada em certificados contribui para o controle de acesso, garantindo que dispositivos que não cumpram os requisitos de segurança não consigam se conectar à rede ou aos sistemas da organização.

- **Criptografia de Dados**.

1. Exigir que dados armazenados em dispositivos e transmitidos pela rede sejam criptografados.

A criptografia de dados representa uma das técnicas mais eficazes para a proteção de informações sensíveis, tanto em repouso (armazenamento) quanto em trânsito (transmissão). Exigir a criptografia de dados armazenados nos dispositivos BYOD assegura que, em caso de perda ou roubo de dispositivos, as informações permaneçam protegidas. De maneira semelhante, a criptografia da comunicação em redes externas, como redes Wi-Fi públicas, protege os dados durante o trânsito, prevenindo interceptações por agentes maliciosos.

2. Implementar VPNs para proteger a comunicação em redes externas.

Uma prática comum associada à criptografia é a implementação de Redes Privadas Virtuais (VPN - *Virtual Private Network*), que estabelecem uma conexão segura entre o dispositivo BYOD e a rede corporativa, garantindo a integridade e a confidencialidade dos dados transmitidos, especialmente em ambientes externos.

- **Segmentação de Rede e Firewalls**.

1. Configuração de VLANs para segmentar o tráfego BYOD e limitar os recursos acessíveis.

   A segmentação de rede é uma técnica utilizada para dividir a infraestrutura de rede em segmentos distintos, de modo a limitar o acesso e a exposição dos recursos a diferentes tipos de tráfego, incluindo o gerado pelos dispositivos BYOD. A utilização de VLANs (Redes Locais Virtuais) constitui uma estratégia eficaz, pois permite isolar o tráfego proveniente de dispositivos pessoais de outros segmentos da rede corporativa, assegurando que os usuários de dispositivos BYOD tenham acesso restrito apenas aos recursos aos quais estão autorizados.

2. Utilização de *firewalls* para filtrar tráfego e bloquear acessos não autorizados.

   Um *firewall* é um mecanismo de segurança que estabelece um ponto de controle ou bloqueio entre uma rede interna segura e uma rede externa considerada não confiável, como a Internet. Sua principal função é permitir o tráfego autorizado entre essas redes, ao mesmo tempo em que restringe ou bloqueia acessos não autorizados à rede interna.

   Em contextos corporativos, é comum o uso de *firewalls* para proteger a conexão entre a rede interna da empresa e a Internet, embora também seja possível empregar um *firewall* para proteger diferentes redes internas entre si. O *firewall* atua como um ponto único de filtragem (*"chokepoint"*), onde o tráfego é monitorado e controlado conforme as políticas de segurança definidas pela organização. As principais funções de um *firewall* incluem:

   – Permitir que os usuários da rede interna acessem recursos externos autorizados;
   – Impedir que usuários não autorizados provenientes da rede externa acessem recursos da rede interna.

   De maneira análoga, o *firewall* não apenas controla o tráfego de entrada e saída da rede, mas também monitora os dados que transitam por ele, fornecendo um meio de detectar e mitigar atividades maliciosas ou não autorizadas que possam ocorrer dentro da rede interna.

   Ademais, a implementação de *firewalls* é fundamental para monitorar e filtrar o tráfego de rede, bloqueando acessos não autorizados e detectando tentativas de intrusão. Os *firewalls* desempenham um papel fundamental na manutenção da segurança da rede, mitigando o risco de penetração de tráfego malicioso ou não autorizado na infraestrutura organizacional.

- **Análise de Comportamento de Tráfego**.

1. Uso de ferramentas de análise para identificar padrões de uso suspeitos ou anômalos.

   A utilização de ferramentas para análise de comportamento de tráfego é essencial para monitorar o uso da rede em tempo real e identificar padrões anômalos ou suspeitos de tráfego. Tais ferramentas permitem a detecção de atividades que fogem dos comportamentos esperados, como tentativas de acesso não autorizado ou comunicações com endereços IP desconhecidos ou suspeitos.

2. Implementação de IDS/IPS (sistemas de detecção/prevenção de intrusões) para proteção ativa.

   A implementação de IDS/IPS (Sistemas de Detecção/Prevenção de Intrusões) é outra técnica importante, visto que esses sistemas são capazes de identificar e bloquear ataques em tempo real, impedindo comprometimentos de segurança antes que causem danos significativos. A combinação de análise de tráfego com sistemas IDS/IPS proporciona uma camada adicional de proteção contra ameaças externas e internas, permitindo uma resposta proativa e eficiente a incidentes de segurança.

- **Patch Management e Atualizações Forçadas**.

1. Exigir que dispositivos mantenham sistemas operacionais e aplicativos atualizados.

   Patch Management é o processo de aplicação de atualizações emitidas pelo fornecedor para fechar vulnerabilidades de segurança e otimizar o desempenho de *softwares* e dispositivos. A técnica consiste em equilibrar a cibersegurança com as necessidades operacionais organizacional. A gestão de *patches* e a aplicação de atualizações forçadas são componentes essenciais de qualquer estratégia de segurança para dispositivos BYOD. Garantir que sistemas operacionais e aplicativos dos dispositivos pessoais estejam sempre atualizados é uma prática fundamental para evitar vulnerabilidades que possam ser exploradas por agentes maliciosos. A atualização regular de *software* assegura que falhas de segurança sejam corrigidas rapidamente, minimizando o risco de ataques.

2. Bloquear dispositivos com versões obsoletas ou vulneráveis.

   Uma medida adicional relevante nesse contexto é a exigência de que os dispositivos realizem atualizações automáticas ou a restrição de acesso à rede corporativa para dispositivos que não atendam aos requisitos de atualização. Isso impede que dispositivos obsoletos, e portanto vulneráveis, acessem recursos corporativos, reduzindo significativamente os riscos de comprometimento da segurança.

Essas técnicas, quando implementadas de maneira integrada e coordenada, constituem uma estratégia robusta para permitir a adoção de políticas BYOD sem comprometer a segurança dos dados e dos sistemas corporativos. De maneira resumida, a Tabela 2 sintetiza as técnicas, dividindo-as em categorias principais e destacando os pontos mais relevantes.

Técnica	Descrição
Segregação de Dados e Aplicativos	Uso de contêineres ou *sandboxes* para isolar dados corporativos dos pessoais, garantindo que aplicativos corporativos funcionem de forma independente dos pessoais. Contêineres e *sandboxes* proporcionam ambientes isolados e seguros para dados e aplicativos corporativos.
Autenticação e Controle de Acesso	Implementação de autenticação multifator (MFA), combinando fatores de conhecimento, posse e inerentes para proteger o acesso. Uso de certificados digitais para autenticar dispositivos e garantir acesso apenas a dispositivos autorizados.
Criptografia de Dados	Criptografia de dados armazenados e em trânsito para proteger informações sensíveis. Uso de VPNs para garantir conexões seguras entre dispositivos BYOD e a rede corporativa.
Segmentação de Rede e Firewalls	Configuração de VLANs para segmentar o tráfego BYOD, limitando o acesso a recursos corporativos. Utilização de *firewalls* para monitorar, filtrar tráfego e bloquear acessos não autorizados.
Análise de Comportamento de Tráfego	Uso de ferramentas para identificar padrões de tráfego suspeitos ou anômalos. Implementação de IDS/IPS para detectar e prevenir intrusões, protegendo ativamente a rede.
Patch Management e Atualizações Forçadas	Implementação de atualizações automáticas e restrição de acesso a dispositivos desatualizados. Bloqueio de dispositivos com versões obsoletas ou vulneráveis para minimizar riscos e garantir a conformidade com as políticas de segurança.

Tabela 2 – Técnicas para Mitigação de Riscos no BYOD

7 CONCLUSÃO

Este estudo apresentou uma revisão da literatura que aborda as principais estratégias de mitigação de riscos em ambientes BYOD. Para atingir esse objetivo, apresentamos as principais práticas adotadas por organizações que adotam a gestão de dispositivos BYOD com base na literatura existente. O objetivo da apresentação das principais técnicas foi o desenvolvimento de recomendações práticas para aprimorar as estratégias de mitigação de riscos em relação a evolução constante das ameaças digitais. O estudo também oferece diretrizes para organizações que desejam implementar ou aprimorar as políticas de BYOD em suas organizações de forma eficiente.

O estudo demonstrou que à adesão ao BYOD, impacta positivamente nos resultados das organizações, promovendo aumento nas taxas de produtividade das empresas, tendo em vista que a adesão ao BYOD proporciona uma maior flexibilidade, mobilidade, afinidade dos colaboradores com o dispositivo utilizado na execução de suas atividades operacionais. Conclui-se que a adesão ao BYOD oferece as empesas benefícios financeiros como, a redução nos custos de aquisição, manutenção e suporte dos dispositivos, além de uma atualização tecnológica.

Uma limitação observada no estudo é que, apesar de os benefícios do BYOD, como aumento da produtividade e redução de custos com aquisição e manutenção de dispositivos, terem sido apresentados, não foi possível mensurar de forma precisa o impacto dos riscos associados a essa prática, especialmente no que se refere à segurança da informação e à proteção de dados sensíveis. Além disso, a investigação não conseguiu avaliar adequadamente a eficácia das medidas de conscientização e treinamento implementadas, uma vez que a conscientização do usuário e a responsabilidade sobre a proteção dos dispositivos e dados corporativos ainda são áreas que necessitam de melhorias. Essa limitação pode afetar a compreensão completa do equilíbrio entre os benefícios e os riscos do BYOD nas organizações.

O estudo realizado na COGETI-TD, investigou as estratégias e políticas existentes na instituição para mitigar os riscos associados ao uso do BYOD. A investigação conclui que, embora não exista uma política formal definida sobre BYOD, a organização adota alguns mecanismos que contribuem para a redução dos riscos relacionados a essa prática. No entanto, a investigação revela que ainda há áreas que demandam melhorias, particularmente no que se refere à conscientização dos usuários e à sua responsabilidade na proteção dos dispositivos e dos dados corporativos nele armazenados. Ademais, destaca-se a ausência de uma política estruturada de educação e treinamento continuo, essencialmente para promover a conscientização dos usuários quanto aos riscos inerentes ao BYOD.

Como recomendação para um trabalho futuro, poderia ser realizado um estudo aprofundado em uma instituição que adote uma política formal de BYOD, com o objetivo de analisar as práticas de gestão e mitigação de riscos relacionadas ao uso de dispositivos pessoais no ambiente corporativo. A pesquisa deverá focar na avaliação da estrutura da política de BYOD, na implementação de medidas de segurança, e na conscientização dos colaboradores sobre os

riscos envolvidos. Com base nos resultados obtidos, podem ser desenvolvidas novas recomendações práticas para aprimorar as estratégias de segurança e gestão de dispositivos móveis, incluindo a definição de políticas claras, o uso de ferramentas de monitoramento e controle, além de programas de treinamento contínuo. Esse estudo permitirá não apenas entender a aplicação do BYOD em um contexto mais amplo, mas também contribuir para a formulação de boas práticas que possam ser replicadas em outras organizações, promovendo um ambiente de trabalho mais seguro e eficiente.

REFERÊNCIAS

(ABNT), A. B. de N. T. **ABNT NBR ISO 31000:2018 - Gestão de riscos–Princípios e diretrizes**. [*s.n.*], 2018. Disponível em: https://www.abntcatalogo.com.br/norma.aspx?ID=339044.

ALMEIDA, R. N. d. Estelionato virtual no direito brasileiro. Pontifícia Universidade Católica de Goiás, 2023.

ARAÚJO, T. M. d.; LUA, I. O trabalho mudou-se para casa: trabalho remoto no contexto da pandemia de covid-19. **Revista Brasileira de Saúde Ocupacional**, SciELO Brasil, v. 46, 2021.

BARBOSA, G. A. R.; BARRIVIERA, M. H. *et al.* Segurança da informação: A proteção contra o vazamento de dados e sua importância para as empresas privadas. **Revista Eletrônica e-Fatec**, v. 6, n. 1, p. 10–10, 2016.

BOIARSKI, J. A. *et al.* **Caracterização do uso de dispositivos móveis particulares nos Câmpus do sudoeste da UTFPR: subsídios para a construção de uma política de BYOD**. 2018. Dissertação (Mestrado) — Universidade Tecnológica Federal do Paraná, 2018.

BRADLEY, J. *et al.* **BYOD: A Global Perspective - Harnessing Employee-Led Innovation**. 2012. Disponível em: https://www.cisco.com/c/dam/en_us/about/ac79/docs/re/BYOD_Horizons-Global.pdf.

CERT.br. **Cartilha de Segurança para Internet**. [*S.l.*], 2012. Acessado em: 10 ago. 2024. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf.

COTO, I.; DIAS, P. V. R. Bring your own device (byod): Quais as vantagens e desvantagens que podem ter nas organizações no contexto de segurança da informação. **Educamazônia-Educação, Sociedade e Meio Ambiente**, v. 16, n. 2, jul-dez, p. 497–510, 2023.

DORNELES, D. de M.; ROHDEN, R. B.; TELOCKEN, A. V. Ataques cibernéticos usando engenharia social. **REVISTA INTERDISCIPLINAR DE ENSINO, PESQUISA E EXTENSÃO**, v. 9, n. 1, p. 68–81, 2021.

EKE, C. I.; ANIR, A. N. Bring your own device (byod) security threats and mitigation mechanisms: Systematic mapping. *In*: IEEE. **2021 International Conference on Computer Science and Engineering (IC2SE)**. [*S.l.*], 2021. v. 1, p. 1–10.

FONTES, E. L. G.; BALLONI, A. J.; LAUDON, K. C. A segurança de sistemas da informação: aspectos sociotécnicos. **A SEGURANÇA DE SISTEMAS DA INFORMAÇÃO: ASPECTOS SOCIOTÉCNICOS..... 5**, 2015.

GARBA JOCELYN ARMAREGO, D. M. A. B.; KENWORTHY, W. Review of the information security and privacy challenges in bring your own device (byod) environments. **Journal of Information Privacy and Security**, Routledge, v. 11, n. 1, p. 38–54, 2015.

HINTZBERGEN, J. *et al.* **Fundamentos de Segurança da Informação: Com base na ISO 27001 e na ISO 27002**. [*S.l.*]: Brasport, 2018.

IBM. **O que é engenharia social?** 2023. Acessado em: 18-ago-2024. Disponível em: https://www.ibm.com/br-pt/topics/social-engineering?mhsrc=ibmsearch_a&mhq=engenharia%20social.

IBM. **O que é a segurança da informação?** 2024. Acessado em: 07/03/2024. Disponível em: https://www.ibm.com/br-pt/topics/information-security.

International Organization for Standardization (ISO). **ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary**. [*S.l.*]: ISO, 2018. ISO standard.

ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management. 2005. International Organization for Standardization. ISO/IEC 17799:2005. Genebra: ISO/IEC, 2005.

ISO/IEC 27032:2012 - Information technology - Security techniques - Guidelines for cybersecurity. 2012. International Organization for Standardization. Https://www.iso.org/standard/44375.html.

JERO, S. *et al.* Practical principle of least privilege for secure embedded systems. *In*: IEEE. **2021 IEEE 27th Real-Time and Embedded Technology and Applications Symposium (RTAS)**. [*S.l.*], 2021. p. 1–13.

KIM, D.; SOLOMON, M. G. **Fundamentos de segurança de sistemas de informação**. Rio de Janeiro: LTC, 2014. 386 p.

KITCHENHAM, B.; BRERETON, P. A systematic review of systematic review process research in software engineering. **Information and software technology**, Elsevier, v. 55, n. 12, p. 2049–2075, 2013.

KONZEN, M. P. *et al.* Gestão de riscos de segurança da informação baseada na norma nbr iso/iec 27005 usando padrões de segurança. Universidade Federal de Santa Maria, 2013.

NIST. **Guidelines for Managing the Security of Mobile Devices in the Enterprise**. [*S.l.*], 2013. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r2.pdf.

NIST. **Security and Privacy Controls for Information Systems and Organizations**. [*S.l.*], 2020. Disponível em: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

OLIVEIRA, M. S. *et al.* Aplicaçao das normas abnt nbr iso/iec 27001 e abnt nbr iso/iec 27002 em uma média empresa. **Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica**, v. 6, n. 2, 2016.

PETERSEN, K. *et al.* Systematic mapping studies in software engineering. *In*: BCS LEARNING & DEVELOPMENT. **12th international conference on evaluation and assessment in software engineering (EASE)**. [*S.l.*], 2008.

RATCHFORD, M. *et al.* Byod security issues: A systematic literature review. **Information Security Journal: A Global Perspective**, Taylor & Francis, v. 31, n. 3, p. 253–273, 2022.

SOOMRO, Z. A.; SHAH, M. H.; AHMED, J. Information security management needs more holistic approach: A literature review. **International journal of information management**, Elsevier, v. 36, n. 2, p. 215–225, 2016.

STAPLETON, J. J. **Security without obscurity: A guide to confidentiality, authentication, and integrity**. [*S.l.*]: CRC press, 2014.