INTERFACE TECNOLÓGICA

DISPOSITIVOS PESSOAIS NO TRABALHO: riscos ciberneticos

PERSONAL DEVICES AT WORK: cybersecurity risks

Joao Vitor Tota Fermino – joaovfermino1250@gmail.com
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – SP – Brasil

Elton Batistão – elton.batistao@fatec.sp.gov.br
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – SP – Brasil

DOI: 10.31510/infa.v22i2.2340
Data de submissão: 25/09/2025
Data do aceite: 09/12/2025
Data da publicação: 20/12/2025

RESUMO

O uso de dispositivos pessoais em ambientes corporativos, prática conhecida como Bring Your Own Device (BYOD), tornou-se cada vez mais comum diante da mobilidade e da flexibilidade exigidas pelo mercado atual. No entanto, essa tendência amplia a superfície de ataque e expõe organizações a novos riscos cibernéticos. Este artigo discute as principais vulnerabilidades relacionadas ao uso de smartphones, tablets e laptops pessoais no trabalho, analisa as ameaças decorrentes dessa prática e propõe diretrizes para mitigar os impactos, considerando aspectos técnicos, gerenciais e culturais. Os resultados sugerem que políticas de segurança bem definidas, aliadas a soluções tecnológicas e à conscientização contínua dos colaboradores, são fundamentais para equilibrar produtividade e proteção da informação sensível.

Palavras-chave: BYOD. Cibernéticos. Segurança. Dispositivos.

ABSTRACT

The use of personal devices in corporate environments, a practice known as Bring Your Own Device (BYOD), has become increasingly common due to the mobility and flexibility demanded by today's market. However, this trend expands the attack surface and exposes organizations to new cybersecurity risks. This article discusses the main vulnerabilities related to the use of

personal smartphones, tablets, and laptops at work, analyzes the threats arising from this practice, and proposes guidelines to mitigate their impacts, considering technical, managerial, and cultural aspects. The findings suggest that well-defined security policies, combined with technological solutions and continuous employee awareness, are essential to balance productivity and the protection of sensitive information.

Keywords: BYOD. Cybersecurity. Security. Device.

1 INTRODUÇÃO

O uso de celulares, tablets e notebooks pessoais no ambiente de trabalho, prática conhecida como *Bring Your Own* Device (BYOD), tem se tornado cada vez mais comum nas empresas. Essa tendência, chamada também de *consumerização da TI*, traz benefícios como agilidade e praticidade para os colaboradores, mas também cria novos desafios para a segurança da informação. Como alerta uma pesquisa da *Proofpoint* (2013), "o maior risco para as empresas é não acompanhar este movimento. Independentemente de qualquer medida da organização, os colaboradores em geral estão usando dispositivos móveis pessoais dentro do ambiente de trabalho". Essa realidade mostra que não basta tentar impedir o uso desses aparelhos: é preciso entender seus impactos e adotar medidas adequadas.

O problema que este artigo busca investigar é quais riscos cibernéticos surgem quando os funcionários utilizam seus próprios dispositivos para fins profissionais e como isso pode afetar a proteção dos dados corporativos. O objetivo principal é analisar esses riscos e apresentar práticas que ajudem a reduzir vulnerabilidades, apoiando as empresas na criação de políticas mais seguras para o uso de dispositivos pessoais.

A relevância do estudo está no fato de que, em um cenário cada vez mais digital, falhas no controle do BYOD podem gerar vazamento de informações, prejuízos financeiros e problemas legais. Assim, compreender o fenômeno é essencial para que as organizações equilibrem produtividade e segurança.

Para atingir esses objetivos, será feita uma pesquisa exploratória, baseada em revisão bibliográfica e análise de documentos, relatórios e estudos de caso sobre BYOD e segurança cibernética.

Parte-se da hipótese de que empresas que criam políticas claras, aliadas a boas práticas de gestão e conscientização dos colaboradores, conseguem reduzir significativamente os riscos ligados ao uso de dispositivos pessoais no trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

Com a análise feita, ficou claro que o uso de dispositivos pessoais no trabalho traz muitos riscos para as empresas. Entre os principais estão o uso de redes wi-fi inseguras, a chance de infecção por malware e ransomware, além do roubo dos aparelhos, que pode levar ao vazamento de dados importantes. Esses pontos confirmam que o BYOD precisa de regras bem definidas, senão a segurança da informação fica comprometida.

Também foi possível perceber que não adianta simplesmente proibir os colaboradores de usar seus próprios aparelhos, já que essa prática já faz parte da realidade das empresas. O que realmente ajuda é ter soluções como o gerenciamento de dispositivos móveis (MDM), a segmentação da rede e, principalmente, o treinamento dos funcionários para reconhecer ameaças e agir de forma mais segura.

Outro ponto importante é que a segurança precisa caminhar junto com o respeito à privacidade do colaborador. Ou seja, a empresa deve adotar políticas claras, mas que também sejam justas e transparentes. Assim, os resultados mostram que a combinação de tecnologia, normas e conscientização é o que torna possível reduzir os riscos e manter o equilíbrio entre produtividade e proteção dos dados.

2.1 BRING YOUR OWN DEVICE (BYOD)

O modelo de trabalho conhecido como "*Bring Your Own Device*" (BYOD) representa uma mudança significativa na cultura corporativa. Ele incentiva que os profissionais usem seus próprios dispositivos, de laptops a celulares, para executar suas tarefas diárias. A principal atração para as empresas reside na economia com a compra e gestão de equipamentos, enquanto os colaboradores se beneficiam da familiaridade e do conforto de suas próprias ferramentas tecnológicas.

Diante desse risco elevado, a segurança em BYOD torna-se fundamental para garantir a proteção, a precisão e o acesso contínuo às informações do negócio. A implementação de uma política de segurança sólida é o caminho para mitigar essas ameaças. Medidas como criptografia de ponta a ponta, senhas fortes com verificação em duas etapas e a limitação de acesso apenas ao que é necessário para cada função são essenciais.

A segurança do BYOD não deve ser vista como um obstáculo, ao aplicar boas práticas e treinamentos adequados, as empresas podem usufruir muito das vantagens da mobilidade e diminuindo muito o risco de ataques.

2.2 IMPORTÂNCIA DA SEGURANÇA BYOD

Adotar o BYOD traz consigo uma responsabilidade inescapável: proteger a informação corporativa em dispositivos que não pertencem à empresa. Cada aparelho pessoal conectado à rede se torna um novo ponto de vulnerabilidade. A perda de um aparelho ou o uso de uma rede de internet desprotegida em um café, por exemplo, pode se transformar em um grave incidente de vazamento de dados confidenciais.

Diante desse risco elevado, a segurança em BYOD torna-se fundamental para garantir a proteção, a precisão e o acesso contínuo às informações do negócio. A implementação de uma política de segurança sólida é o caminho para mitigar essas ameaças. Medidas como criptografia de ponta a ponta, senhas fortes com verificação em duas etapas e a limitação de acesso apenas ao que é necessário para cada função são essenciais.

É igualmente crucial educar os colaboradores, transformando-os em aliados na proteção dos dados. Em última análise, uma estrutura de segurança em BYOD bem implementada não freia a inovação; pelo contrário, ela a habilita, permitindo que a empresa desfrute com tranquilidade de todos os benefícios da mobilidade e da flexibilidade.

2.3 PRINCIPAIS RISCOS CIBERNETICOS

> Segundo dados do IBGE, “o percentual de brasileiros que trabalham em seu domicílio de residência é de 8,3% do total. A parcela até teve uma ligeira queda em relação a 2022, quando eram 8,5%. Mas segue como tendência firme após a pandemia de Covid. Para se ter uma ideia, em 2019, eram só 5,8% nesta situação” (CASTRO, 2024).

Com o aumento do número de trabalhadores em home office, cresce também a quantidade de profissionais que utilizam seus próprios dispositivos digitais para executar tarefas corporativas, o que amplia os desafios relacionados à segurança da informação, segue a baixo os principais riscos enfrentados pelas empresas.

2.3.1 Redes Wi-fi inseguras

As redes wi-fi possuem um enorme risco, principalmente se for rede wi-fi publica, como em shopping, aeroporto ou cafeterias, na maioria das vezes elas são desprotegidas ou não possuem segurança. Uma pessoa mal intencionada pode se posicionar entre seu dispositivo e o ponto de acesso wi-fi, criando o que chamamos de ataque man-in-the-middle, nesse ataque, toda comunicação entre, senhas, e-mails e documentos podem ser interceptados.

2.3.2 Malware e Ransomware

A segurança e os softwares de proteção em dispositivos pessoais são mais fracos ou inexistentes, o funcionário pode baixar um aplicativo não oficial para o seu celular ou visitar um site de streaming não seguro em seu notebook. Um único clique em um anúncio malicioso pode instalar um spyware que rouba credenciais corporativas, ou um ransomware que criptografa não apenas os arquivos pessoais, mas também os arquivos de trabalho armazenados no dispositivo ou em serviços de nuvem sincronizados.

2.2.3 Roubo de dispositivos

Dispositivos pessoais, como smartphones e notebooks e tablets, são levados para todos lugares, se nesses aparelhos possuir dados corporativos, e for roubado, caso não tenha criptografia ou a capacidade de apagar o conteúdo do aparelho de forma remota, os dados confidenciais podem ser acessados, gerando um roubo de informações e vazamento de dados.

2.2.4 Vazamento de dados

Esse é o resultado final e mais temido de todos os riscos do BYOD, um único ponto fraco em qualquer um dos tópicos acima pode levar a um vazamento, e com isso a falta de controle sobre os dispositivos pessoais cria um terreno fértil para que dados confidenciais sejam perdidos, roubados ou expostos.

3 PROCEDIMENTOS METODOLÓGICOS

Este estudo é fundamentado por meio de pesquisas bibliográficas e de campo, para entender os riscos cibernéticos na era dos dispositivos pessoais no trabalho. O objetivo foi mergulhar na realidade da empresa e de seus colaboradores para compreender como incidentes de segurança acontecem e quais são seus verdadeiros impactos.

Os dados foram obtidos por meio de entrevistas informais com gestores e colaboradores da empresa estudada. Análise documental (políticas internas de segurança, registros bancários e logs de - acesso). E observação direta dos procedimentos adotados após o incidente.

3.1 Procedimento de análise

O material coletado por meio de entrevistas, análise de documentos e observação direta, foi submetido a um rigoroso processo de análise de conteúdo. O objetivo era identificar e classificar os principais riscos que levaram ao incidente, como a engenharia social, a falta de gestão de dispositivos móveis e a pouca conscientização em segurança. Em seguida, cada vulnerabilidade foi detalhada, e as soluções propostas foram estruturadas com base nos controles e nas recomendações de segurança das normas internacionais ISO/IEC 27001 e do NIST, fornecendo um plano de ação robusto e alinhado com as diretrizes do setor.

4. RESULTADOS E DISCUSSÃO

Com a análise feita, ficou claro que o uso de dispositivos pessoais no trabalho traz muitos riscos para as empresas. Entre os principais estão o uso de redes wi-fi inseguras, a chance de infecção por malware e ransomware, além do roubo dos aparelhos, que pode levar ao vazamento de dados importantes. Esses pontos confirmam que o BYOD precisa de regras bem definidas, senão a segurança da informação fica comprometida.

Também foi possível perceber que não adianta simplesmente proibir os colaboradores de usar seus próprios aparelhos, já que essa prática já faz parte da realidade das empresas. O que realmente ajuda é ter soluções como o gerenciamento de dispositivos móveis (MDM), a segmentação da rede e, principalmente, o treinamento dos funcionários para reconhecer ameaças e agir de forma mais segura.

Outro ponto importante é que a segurança precisa caminhar junto com o respeito à privacidade do colaborador. Ou seja, a empresa deve adotar políticas claras, mas que também sejam justas e transparentes. Assim, os resultados mostram que a combinação de tecnologia, normas e conscientização é o que torna possível reduzir os riscos e manter o equilíbrio entre produtividade e proteção dos dados.

4.1 MÉTODOS PARA MITIGAR RISCOS CIBERNÉTICOS EM DISPOSITIVOS PESSOAIS NO TRABALHO

Política de Uso Aceitável é um componente crucial de qualquer estratégia de segurança da informação, nela é fundamental definir os critérios claros para o acesso e a manipulação dos dados organizacionais. Isso assegura que todos os usuários sigam um padrão de conduta que protege a integridade e a confidencialidade das informações da organização.

4.1.1 Gerenciamento de dispositivos móveis (MDM)

Essa implementação é fundamental para a proteção de dados em ambientes de trabalho híbridos. Essas ferramentas oferecem funcionalidades como o controle remoto dos aparelhos, a criptografia de informações sensíveis, a possibilidade de limpar dados de forma seletiva e a aplicação centralizada de políticas de senha para garantir a conformidade e a segurança dos dispositivos.

4.1.2 Segmentação de rede

A segmentação de rede é um pilar da segurança da informação, especialmente em redes que permitem o uso de dispositivos pessoais. Essa técnica cria zonas isoladas para esses aparelhos, limitando seu acesso apenas a recursos específicos. O objetivo principal é minimizar a superfície de ataque e garantir que falhas de segurança em um dispositivo não comprometam a integridade dos sistemas mais importantes da empresa.

4.1.3 Educação e conscientização

Para garantir a segurança da informação no ambiente de trabalho remoto, é essencial investir em treinamento de conscientização. Este tipo de formação tem como principal objetivo dar aos funcionários as ferramentas para reconhecer e neutralizar riscos digitais. O programa deve ser completo, ensinando sobre os perigos do *phishing*, as manobras de engenharia social e a importância de gerir senhas fortes. Educar a equipe sobre como se comportar no mundo digital é a melhor forma de reduzir a chance de erros que podem levar a uma brecha de segurança. Em última análise, uma equipe bem informada é o principal escudo contra ciberataques.

4.1.4 Aspectos legais e éticos

A gestão de dispositivos pessoais no ambiente de trabalho por meio do BYOD, exige atenção aos aspectos legais e éticos. Para isso, é vital que as políticas de segurança não violem a privacidade dos funcionários, adotando uma abordagem não invasiva. O estabelecimento de contratos e termos de uso bem definidos é a melhor forma de proteger a organização e, ao mesmo tempo, preservar os direitos individuais dos colaboradores.

5 CONSIDERAÇÕES FINAIS

A adoção do modelo *Bring Your Own Device* (BYOD) demonstra ser um caminho inevitável para organizações que buscam flexibilidade e agilidade, mas também evidencia a necessidade de um olhar estratégico sobre a segurança da informação. Os riscos analisados, desde redes Wi-Fi inseguras até o vazamento de dados decorrente do uso inadequado de dispositivos pessoais, mostram que a proteção corporativa não depende apenas de ferramentas tecnológicas, mas de políticas bem estruturadas e da participação ativa dos colaboradores.

A experiência estudada reforça que a combinação de controles técnicos, normas claras e capacitação contínua é a forma mais eficaz de reduzir vulnerabilidades. A criação de ambientes segmentados, o uso de soluções de gerenciamento de dispositivos móveis, a definição de termos de uso e o respeito à privacidade dos profissionais formam um ecossistema capaz de equilibrar produtividade e segurança.

Assim, o BYOD não deve ser visto apenas como um desafio, mas como uma oportunidade para amadurecer práticas de governança, fortalecer a cultura de proteção de dados e alinhar a atuação das pessoas e da tecnologia em prol da resiliência organizacional.

REFERÊNCIAS

SENTINELONE; **18 Remote Working Security Risks in Business.** Disponível em: <https://www.sentinelone.com/cybersecurity-101/cybersecurity/remote-working-security-risks/#18-remote-working-security-risks>. Acesso em: 15 set. 2025.

GRUSTNIY, Leonid. Kaspersky, kaspersky daily; **Dispositivos pessoais no trabalho**. 8 de ago. 2019. Disponível em: <https://www.kaspersky.com.br/blog/personal-devices-at-work/12181>. Acesso em: 15 set. 2025.

IBM; **O que é trazer seu próprio dispositivo (BYOD)**. Disponível em: <https://www.ibm.com/br-pt/think/topics/byod>. Acesso em 16 set. 2025.

OFFICETOTA; BYOD; o que é, benefícios, riscos e como implementar. Disponível em: <https://www.officetotal.com.br/blog/byod>. Acesso em 16.set. 2025.

CASTRO, Mayra. O globo. O GLOBO 100; **Trabalhar de casa segue como tendência pós pandemia**. Rio de janeiro, 21 Jun. 2024. Disponível em: <https://oglobo.globo.com/economia/noticia/2024/06/21/trabalhar-de-casa-segue-como-tendencia-pos-pandemia-88percent-dos-brasileiros-atuam-assim-mostra-ibge.ghtml?utm_source=chatgpt.com>. Acesso em 16 set. 2025.

SEBASTIÃO DE BARROS, Mauricio; CAVALLERI DE SOUZA, Michael. Uso de Dispositivos Pessoais no Ambiente de Trabalho: A Relação Colaborador e Empresa. **Direito & TI**, *[S. l.]*, v. 1, n. 8, p. 7, 2017. DOI: 10.63451/ti.v1i8.77. Disponível em: https://direitoeti.com.br/direitoeti/article/view/77. Acesso em: 17 set. 2025.

UNTANGLEBRASIL; Os perigos da BYOD para segurança da sua empresa, Disponivel em: <https://www.untanglebrasil.com.br/os-perigos-da-byod-para-a-seguranca-de-sua-empresa>. Acesso em 22 set. 2025.