DOI: 10.5748/19CONTECSI/PSE/ITM/6992

ADOÇÃO DE BYOD E SHADOW IT: UM ESTUDO DE CASO QUANTO À PERCEPÇÃO E USO RELACIONADO A RISCOS E OPORTUNIDADES EM UMA EMPRESA DO SETOR DE VENDA DE AUTOMÓVEIS

Will Ribamar Mendes Almeida ; https://orcid.org/0000-0001-5999-7536
Emil Brunner World University

Jackson Ferreira de Sousa ; https://orcid.org/0000-0002-4067-3731
Universidade Ceuma

Gylnara Kylma Feitosa Carvalhêdo Almeida ; https://orcid.org/0000-0001-5993-3874
Emil Brunner World University

Yonara Costa Magalhães ; https://orcid.org/0000-0001-5502-9634
Universidade Ceuma

BYOD AND SHADOW IT ADOPTION: A CASE STUDY ON THE PERCEPTION AND USE RELATED TO RISKS AND OPPORTUNITIES IN A COMPANY IN THE AUTOMOBILE SALES SECTOR

Abstract. To improve the productivity of work activities, many employees adopt technologies in the corporate environment such as software that help them to perform certain tasks, especially those based on the cloud and that use personal devices to access and manipulate organizational data, without the endorsement of IT. Such practices refer to Shadow IT and BYOD and, although they help in carrying out organizational tasks, they can compromise the information security of the organization, the customer and the employee. In this, because they are considered normal practices, they need to be constantly addressed by the organization's IT management so that policies and strategies are defined that help transform risks into opportunities.
Keywords: BYOD, SHADOW IT, Risks, Opportunities.

ADOÇÃO DE *BYOD* E *SHADOW* IT: UM ESTUDO DE CASO QUANTO À PERCEPÇÃO E USO RELACIONADO A RISCOS E OPORTUNIDADES EM UMA EMPRESA DO SETOR DE VENDA DE AUTOMÓVEIS

Resumo. Para melhorar a produtividade das atividades do trabalho muitos colaboradores adotam tecnologias no ambiente corporativo como softwares que os ajudam no cumprimento de determinadas tarefas, principalmente os baseados em nuvem e que utilizam dispositivos pessoais para acessar e manipular dados da organização, sem o aval da TI. Tais práticas referem-se a Shadow IT e BYOD e, embora, ajudem na realização das tarefas organizacionais, podem comprometer a segurança da informação da organização, do cliente e do colaborador. Por serem práticas consideradas normais elas precisam ser tratadas constantemente pela gestão da TI da organização para que sejam definidas políticas e estratégias que ajudem a transformar riscos em oportunidades.
Palavras-chave: BYOD, SHADOW IT, Riscos, Oportunidades.

1. Introdução

O avanço crescente das organizações impulsiona a busca pelo aprimoramento na execução de suas atividades no ambiente corporativo e, ao mesmo tempo, tem aumentado a busca por melhores e mais adequadas tecnologias para que o processo de execução de suas atividades se torne mais eficiente. Assim, esta estratégia tem sido alvo de muitas organizações frentes a concorrência do mercado e ao mundo globalizado por ser um diferencial competitivo, para isso, é tendência cada vez mais comum nas organizações que os funcionários levem seus dispositivos para o trabalho, bem como acessem frequentemente softwares e informações relacionadas ao ambiente de negócio utilizando uma ampla variedade de dispositivos pessoais (*smartphones*, *tablets*, *notebooks* etc.).

Insere-se nesse contexto, o fato da adoção do trabalho remoto ter sido acelerada pelo panorama da COVID-19, o que adicionou um impulso maior nessa tendência que já vinha sendo adotada por algumas organizações, mas que ainda estava restrita a áreas específicas ou às empresas que tinham uma cultura organizacional mais inovadora. Junta-se a isto a dinâmica do próprio mercado e a agilidade que a internet trouxe promovendo mudanças no comportamento da maioria dos profissionais, sendo hoje muito valorizadas pelas organizações características como a proatividade e a capacidade de resolução de problemas de maneira autônoma.

Entretanto, o uso de dispositivos e aplicativos, bem como os dados destes recursos que trafegarão na rede da organização, local ou remotamente, e isto pode não ter sido homologado pelo setor de tecnologia da informação da organização ou não existir políticas bem definidas para isso. Desta forma, o uso desses recursos acaba ficando "invisível" ou "nas sombras".

Nem sempre os colaboradores e funcionários estão aptos ou muita das vezes preparados para receberem essas novas tecnologias para o desenvolvimento de suas tarefas e acabam procurando um caminho alternativo, a seu ver mais fácil, por isso tem se tornado muito comum dentro de empresas que os colaboradores façam o uso de dispositivos pessoais e softwares específicos para aprimorar o processo de realização das suas atividades, sem que haja o conhecimento, autorização ou políticas sobre esta utilização pelo departamento de Tecnologia da Informação (TI) da organização.

Com base neste contexto, ressalta-se a importância e a necessidade de avaliar como as empresas e organizações tem respondido a estas novas demandas e formas de trabalho. Deve-se considerar que *BYOD* e *Shadow* IT podem ajudar a resolver um problema de negócio de forma eficiente, mas também podem causar exposição a riscos. Por isso, a intencionalidade deste trabalho é estudá-las e identificá-las para transformar riscos em oportunidades ao negócio fornecendo à organização o conhecimento destas práticas e subsidiando-as com informações que levem a definir políticas e estratégias adequadas.

Desta forma, buscou-se aqui, apresentar os resultados de uma análise preliminar quanto à percepção e o uso de *BYOD* e *Shadow* IT em uma organização, admitindo-se as duas vertentes: oportunidades e riscos. Para isso, mapeou-se onde *BYOD* e *Shadow* IT estavam ocorrendo na organização, quais os recursos foram utilizados e com qual finalidade, também se verificou se existia concordância e políticas para a utilização destas práticas e, se tais práticas são justificadas pela necessidade do negócio.

Essas práticas e costumes, muita das vezes, não são vistas pelos colaboradores como um risco quanto aos dados e às informações do ambiente de trabalho circulando em dispositivos e software que o departamento de Tecnologia da Informação (TI) não tem conhecimento. Essas práticas podem ser associadas à utilização de dois termos, o *BYOD* e o *Shadow* IT.

Esta análise preliminar visa relacionar posteriormente, as condutas, estratégias e ações adotadas pela organização em relação à Lei Geral de Proteção de Dados e a própria governança de dados, incluso também o fator de segurança.

2. *BYOD* e *SHADOW* IT

O termo *BYOD* (*Bring Your Own Device*, traduzido por "traga seu próprio dispositivo"), de acordo com Gruman (2012), é um fenômeno no qual os funcionários podem levar seus próprios dispositivos móveis para o ambiente organizacional e, desta forma, realizar suas atividades.

Para Andrade et al (2020), o termo *BYOD* refere-se a uma nova tendência global que envolve políticas, serviços e tecnologias que viabilizam os colaboradores no desempenho de atividades profissionais utilizando seus próprios dispositivos e equipamentos, como: *Smartphones*, *Tablets* ou *Notebooks*.

Já a expressão *Shadow IT* ou "TI nas sombras" ou "TI invisível", pode ser compreendida como qualquer solução de TI (serviços em nuvem, soluções desenvolvidas pelo usuário, softwares instalados pelo usuário ou dispositivos adquiridos pelo usuário) utilizada por colaboradores de uma organização para auxiliar na realização das tarefas de trabalho, mas que não conta com a aprovação ou suporte formal do setor responsável pela TI dessa organização.

A autora Ferreira (2019, p. 18), menciona em relação ao *BYOD*, que:

> A adoção desse modelo requer mais atenção em relação à segurança da informação da empresa, pois muitas informações sensíveis estão no dispositivo pessoal do funcionário, e o manuseio incorreto ou exposição desses dados é uma vulnerabilidade grave. Dessa forma, é necessário realizar algumas mudanças quanto à administração da rede e criação de regras para o uso autorizado do dispositivo na organização.

Isto complementa o estudo aqui exposto em relação ao vácuo presente na segurança da informação com a realização dessa prática e na *Shadow IT*.

2.1 Vantagens

Sabendo-se o conceito dessas práticas, é muito pertinente pensar nas vantagens e desvantagens que estas apresentam para os colaboradores e para a própria organização.

Segundo a Nativa (2018), uma das vantagens da prática do *BYOD* "é a utilização de seus próprios equipamentos para realizar atividades de trabalho, pois os funcionários se sentem motivados para finalizar os trabalhos mais rapidamente", que remete a diminuição de custos em equipamentos eletrônicos e manutenção.

Segundo a ANPPD no artigo BYOD & LGPD, "Em grande parte das vezes os equipamentos particulares têm configurações melhores que os das empresas, portanto, quando o colaborador utiliza seus próprios aparelhos, observa-se um crescimento na produtividade, permitindo resultados mais eficazes devido à familiaridade que o colaborador possui", que remete ao alto índice de produtividade. Ambas definições se tornam útil para as empresas quando se fala em mostrar resultados no final do mês.

Quando se fala em vantagens da prática da *Shadow IT*, de acordo com o Lenovo Tech Today (2021), "a empresa consegue até uma porcentagem de redução de custos operacionais com isso. Em vez de buscar um software com licença cara, que seria instalado nas máquinas de todo o setor, o colaborador busca uma opção gratuita ou mais acessível somente para seu uso ou de uma equipe menor", ou seja, até mesmo não querendo os colaboradores diminuem os gastos da empresa buscando uma opção de software gratuito para seu trabalho.

2.2 Desvantagens

Ao adotar essas práticas, uma das desvantagens que se pode citar, segundo o site Nativa (2018) "O principal risco que o *BYOD* traz para as empresas é a falta de segurança. Isso porque, quando são conectados a uma rede de internet, podem ser repassados vírus ou arquivos maliciosos de um dispositivo para outro, por exemplo", ou seja, quando se usa um dispositivo onde o departamento de TI não tem controle e ele não tem nenhum tipo de proteção pode acarretar problemas como este descrito.

Segundo a ANPPD no artigo BYOD & LGPD (2022, p. 3)

> Permitir que os colaboradores utilizem seus próprios aparelhos pode exigir da empresa um investimento necessário em tecnologias de ponta, tais como: ativos para proteção de rede, controle de acesso com link de dados, virtual private network (VPN's), autenticação de dois fatores, dentre outros. Outra questão a ser levada em consideração é a possibilidade do colaborador não possuir equipamento adequado para o desenvolvimento de suas tarefas, necessitando que a empresa faça investimento para, neste caso, oferecer um equipamento para desenvolvimento do trabalho, ficando assim responsável por toda manutenção.

Para o caso da *Shadow IT,* uma das desvantagens é apresentada por Kalendae (2021, p. 1) “a prática do *Shadow IT* pode ser bem prejudicial visto que não se sabe a procedência dos programas instalados indevidamente no computador de um usuário. Esses aplicativos suspeitos podem conter Malwares capazes de acessar as máquinas e vazar dados sigilosos”. Sabe-se que em um computador corporativo é um pouco mais difícil disso acontecer pois um usuário não tem permissão para instalação de software, mas em seu Smartphone ou Notebook a TI não tem esse controle e o vazamento de dados sigilosos é iminente.

Tais práticas, comportamentos e recursos utilizados sem o devido cuidado e gestão, podem trazer grandes riscos e comprometer a segurança das informações, inclusive implicando o vazamento de informações sigilosas e prejuízos enormes para a organização. Por outro lado, também podem ser vistas como oportunidade aos negócios na perspectiva de melhorar a produtividade dos funcionários na realização das tarefas do trabalho. E, isto é corroborado por Monteiro Júnior (2018) quando afirma que existem tantos riscos quanto oportunidades no uso de *Shadow IT* e isto é um desafio às organizações, pois exigem novas abordagens para gerenciar este fenômeno, sendo o ponto de partida obter explicações do porquê ele emerge. Silic e Back (apud KUSSAMA, 2017, p. 14) corrobora citando que “O baixo alinhamento da TI com os processos de negócio é considerada a principal causa do fenômeno *Shadow IT* […]”. Logo, isto requer dos profissionais uma resposta rápida e assertiva quanto a estes riscos e a necessidade de mapear, analisar e definir políticas e ações de modo que a *BYOD* e *Shadow IT* na organização possam ser transformadas de risco para oportunidade.

Em uma pesquisa realizada pela Cisco (2012), ela afirma que 47% dos funcionários nas empresas entrevistadas são oficialmente designados como “profissionais móveis”, mas 60% destes funcionários usam um dispositivo móvel no trabalho, 13% a mais que os considerados oficialmente “profissionais móveis”. O Brasil encontra-se na média dos demais países avaliados.

Segundo o conteúdo abordado na certificação NSE2 da Fortinet (2022)

> O NAC é um dispositivo ou uma máquina virtual que controla o acesso de dispositivos a rede, ele começou como método de autenticação de rede e autorização para dispositivos que entram na rede em conformidade com os padrões IEEE 802.1X, o método de autenticação envolve três elementos, dispositivos do cliente, autenticador e o servidor de autenticação. O autenticador pode ser um switch de rede ou um ponto de acesso sem fio que define o limite entre as redes protegidas e desprotegidas, o cliente envia as credenciais em forma de usuário e senha, certificado digital ou de algum outro modo ao autenticador que encaminha essas credenciais ao servidor, dependendo do resultado da autenticação o autenticador pode bloquear o dispositivo ou permitir seu acesso à rede.

A maioria das organizações adotam esse controle de acesso à rede precavendo a utilização de dispositivos pessoais por parte dos colaboradores. E, é por meio do NAC que o controle de acesso é monitorado, o *BYOD* está presente querendo ou não dentro do ambiente corporativo e as atualizações de segurança obrigatoriamente devem seguir essa evolução, os novos desafios de segurança surgiram por conta do uso desses dispositivos por serem pessoais e não pertencem a empresa e o Serviço Gerenciado de Internet (MIS) não controla o que é executado nestes dispositivos, por exemplo software, antivírus ou aplicativos não seguros.

As organizações que procuram manter um bom relacionamento com os seus funcionários, ouvindo suas opiniões e sugestões, conseguem trabalhar para manter um clima organizacional harmonioso. As informações e conhecimento agregam valor ao ser humano e à organização, o que resulta em vantagem competitiva, e é grande aliada no mundo atual (NAKAMURA, 2007). Para Chiavenato (2008), os colaboradores podem considerados recursos produtivos da organização, e geralmente são passivos, com uniformes e inertes,

necessitando de acompanhamento contínuo dos chefes, quando são tratados como parceiros, estes acabam fornecendo seus conhecimentos, habilidades e competências para a empresa, se esforçando mais e demonstrando maior comprometimento e responsabilidade.

3. Metodologia

Para alcançar os objetivos propostos foi realizado um estudo de caso em uma organização, na qual foi desenvolvida uma pesquisa de campo descritiva e qualitativa sobre as práticas de *BYOD* e *Shadow IT*. Para isso, realizamos as seguintes atividades:

- Revisão de literatura sobre Shadow IT e *BYOD*, conceitos, origem, natureza;
- Caracterização do perfil da organização estudada e a delimitação dos setores e áreas nos quais esta pesquisa será realizada, pois faz-se necessário alinhar o cronograma da pesquisa com o tamanho e porte da organização a ser pesquisada;
- Elaboração e aplicação de questionário de percepção sobre o conhecimento dos colaboradores da organização sobre *BYOD* e *Shadow IT*, tabulando os resultados encontrados e subsidiando a etapa de mapeamento;
- Mapeamento dos recursos (softwares, serviços e dispositivos) mais utilizados na prática de *BYOD* e *Shadow IT*, descrevendo um panorama situacional da organização;
- Análise dos resultados do questionário de percepção, do mapeamento e da situação da organização, indicando riscos e oportunidades existentes.

O projeto de pesquisa foi apresentado aos colaboradores selecionados para participarem da pesquisa, um total de 11 pessoas aceitaram participar. A pesquisa foi realizada no período de 22/08/2021 à 26/08/2021, o meio utilizado para a pesquisa foi o questionário impresso em papel para a coleta de dados e a ferramenta do Canva para fazer os gráficos com os dados coletados na pesquisa.

4. Discussão e resultados alcançados

4.1 Caracterização do perfil da organização

Os dados e informações que serão apresentados neste estudo foram recolhidos do ambiente corporativo de uma empresa que tem como principal atividade, vendas de automóveis novos, vendas de peças genuínas e serviços de oficina localizada na cidade “A”. Esta empresa de venda de automóveis está organizada em 19 (dezenove) setores. A empresa comporta em suas dependências, em média, 66 computadores incluindo Desktops, Notebooks e Star Diagnoses. Também se considerou os dispositivos pessoais dos colaboradores como o celular, que faz parte do estudo realizado.

Para a realização da etapa de Elaboração e Aplicação de questionário de percepção e pesquisa, foram selecionados 7 (sete) setores: Administrativo, Caixa, DVN (Departamento de Veículos Novos), Gerência, Fiscal, Financeiro e Compras, pois nestes setores são realizadas atividades de gestão e administração, e nos quais podem ser fonte de um alto uso das práticas de *BYOD* e *Shadow IT*. Além disso, em tais setores, houve maior disponibilidade de tempo dos colaboradores em participar das entrevistas, por meio das perguntas que compõem o questionário, como também maior facilidade de acesso às informações sobre os sistemas de softwares utilizados e demais equipamentos.

Vale ressaltar que no período em que o questionário estava sendo aplicado os colaboradores foram orientados a responder as perguntas sem medo de qualquer retaliação a seus empregos por parte da organização, gerando assim respostas verdadeiras e valiosas para este estudo. E, para o mapeamento dos recursos, realizou-se a seleção de amostragem dos setores fez-se o levantamento dos equipamentos corporativos utilizados pelos colaboradores para a realização das atividades organizacionais. Quanto ao questionário de percepção, foram

elaboradas 08 perguntas: sendo 2 de múltipla escolha e 6 discursivas. As perguntas que compõem o questionário, foram estruturadas em duas seções: Software e Hardware.

Perguntas sobre os Softwares

1 – Você usa algum software/programa/aplicativo que não faz parte do padrão estabelecido pela TI da empresa, para fazer/auxiliar em suas atividades de trabalho?

2 – Qual(is) o(s) software(s)/programa(s)/aplicativo(s) você usa?

3 – Por que você usa esse(s) software(s)/programa(s)/aplicativo(s)?

4 – Você já teve algum tipo de problema ao usar esse(s) software(s)/programa(s)/aplicativo(s)?

Perguntas sobre os Hardwares

1 – Você usa algum dispositivo físico pessoal para fazer/auxiliar em suas atividades de trabalho?

2 – Qual (is) dispositivo (s) você usa?

3 – Por que você usa esse (s) dispositivo(s)?

4 – Você já teve algum tipo de problema ao usar esse(s) equipamento(s) pessoal(is) em atividades da organização?

Considerando a disponibilidade e a disposição de cada colaborador, as entrevistas foram realizadas no período de 22/08/2021 à 26/08/2021, com um total de 11 pessoas. Sendo 01 do setor Caixa; 02 do setor DVN; 01 do setor Gerência; 03 do setor Administrativo; 01 Fiscal; 02 do setor Financeiro; 01 do setor Compras.

Considerando a importância da visão do departamento de TI da organização, ações e intervenções que são tomadas, conversamos com o supervisor do departamento para que assim possamos compreender melhor a estrutura de segurança da informação da empresa e as medidas tomadas em relação ao BYOD e Shadow IT.

4.2 Mapeamento de recursos

Com a seleção de amostragem dos setores fez-se o levantamento dos equipamentos corporativos utilizados pelos colaboradores para a realização das atividades organizacionais, como demonstrado no Quadro 01, abaixo:

Quadro 1. Levantamento dos equipamentos corporativos utilizados pelos colaboradores

SETOR	DESKTOP	NOTEBOOK	SMARTPHONE
Caixa	1	0	0
DVN	2	0	1
Gerência	0	1	1
Administrativo	2	1	0
Fiscal	1	0	0
Financeiro	2	0	0
Compras	1	0	0
TOTAL		**13**	

O mapeamento dos softwares utilizados está descrito no Quadro 02, a seguir:

Quadro 2. Levantamento dos softwares corporativos utilizados pelos colaboradores

SOFTWARE	DESCRIÇÃO
Navegador Chrome	Navegar na internet
Navegador Firefox	Navegar na internet
Java	Executar aplicações Java
Putty	Conexão com servidores remotos
Ultravnc	Acesso remoto
Anydesk	Acesso remoto
Thunderbird	Cliente\e-mail
Wps Office	Criação e edição de documentos, planilhas e apresentações
Libre Office	Criação e edição de documentos, planilhas e apresentações
Adobe Acrobat	Visualizar PDF
Kaspersky Endpoint	Antivírus
Pacote Office 365	Criação e edição de documentos, planilhas e apresentações. Cliente/e-mail
Zoom	Reunião
Google Meet	Reunião
Whatsapp Business	Aplicativo de mensagens
Navegador Exclusivo Bradesco	Acesso à conta de forma mais segura
TOTAL	**16**

Todos os dispositivos e softwares descritos nos Quadros 01 e 02, acima, são de conhecimento, autorização e instalação do departamento de TI da organização. No Quadro 03 são apresentados os dispositivos e softwares pessoais utilizados:

Quadro 3. Levantamento de Hardware e softwares pessoais

SETOR	DISPOSITIVO	QTD	SOFTWARE	DESCRIÇÃO
Caixa	Smartphone	1	Whatsapp	Aplicativo de mensagem
DVN	Smartphone	2	Whatsapp, Gmail	Aplicativo de mensagens, cliente/e-mail
Gerência	Smartphone	1	Whatsapp, Hotmail	Aplicativo de mensagens, cliente/e-mail
Administrativo	Smartphone	3	Whatsapp, Gmail, Agenda do Google	Aplicativo de mensagens, cliente/e-mail, organizador de tarefas
Fiscal	Smartphone	1	Whatsapp, Câmera	Aplicativo de mensagens, fotografia
Financeiro	Smartphone	2	Whatsapp, Canva	Aplicativo de mensagens/programa para criação e edição
Compras	Smartphone	1	Gmail, Whatsapp, Instagram	Cliente/e-mail, aplicativo de mensagens/rede social
TOTAL	**11**		**15**	

Com os dados recolhidos nas entrevistas utilizando o questionário de percepção, foram feitas algumas análises de quais características mais evidentes que rodeiam os colaboradores que muitas das vezes são práticas consideradas como normais.

4.3 Quanto à prática do *BYOD*

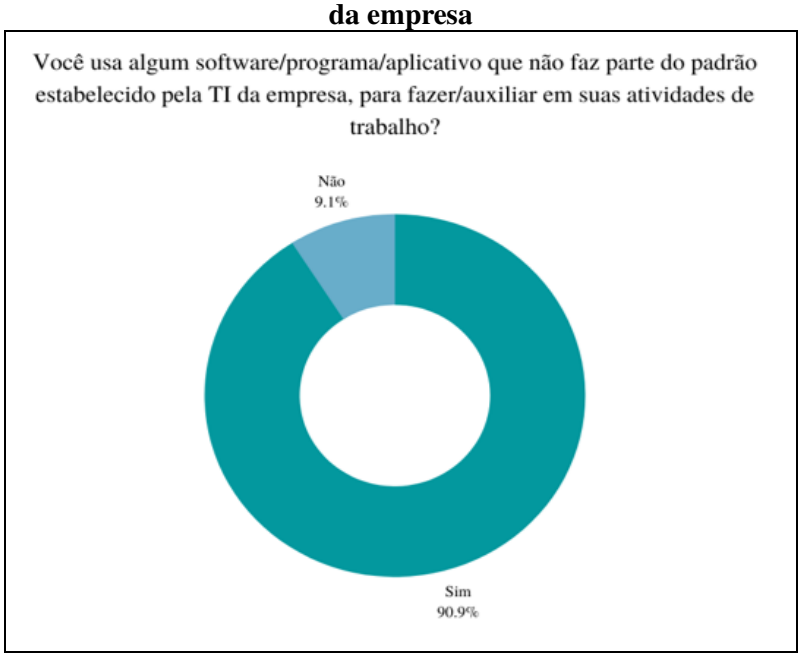
Como resposta da primeira pergunta pôde-se observar que todos os colaboradores usam pelo menos um dispositivo pessoal no ambiente corporativo para auxiliar em suas atividades de trabalho. Na pergunta dois, quando se pergunta qual(is) dispositivo(s) usado durante as atividades os entrevistados responderam: “Celular/Smartphone”.

Já na pergunta três, um dos motivos da escolha do telefone celular pelos colaboradores é a condição financeira para possuir outros dispositivos como notebooks ou *tablets*; o segundo motivo é pela agilidade do uso do telefone para realizar suas atividades de forma rápida e eficiente por estar sempre presente. Em um segundo momento, alguns entrevistados informaram que usam o seu dispositivo pessoal porque a empresa não disponibilizou um corporativo e, também, mencionaram que usam seu dispositivo pessoal porque o corporativo não suporta os aplicativos e programas necessários para suas atividades. Na quarta pergunta, 50% dos entrevistados informaram que nunca tiveram problemas com seus dispositivos na execução de uma atividade e os outros 50%, informaram que tiveram problemas, dentre os quais citaram as seguintes situações: travamento, arquivos não suportados pelo telefone celular, desligou inesperadamente e botões defeituosos.

4.4 Quanto à prática da *Shadow IT*

Em resposta à primeira pergunta foi observado que 91% dos entrevistados usam softwares ou aplicativos para auxiliar em suas tarefas de trabalho com o intuito de melhorar a eficiência nos processos; e, 9%, não usa qualquer software ou aplicativos. Conforme o gráfico 01.

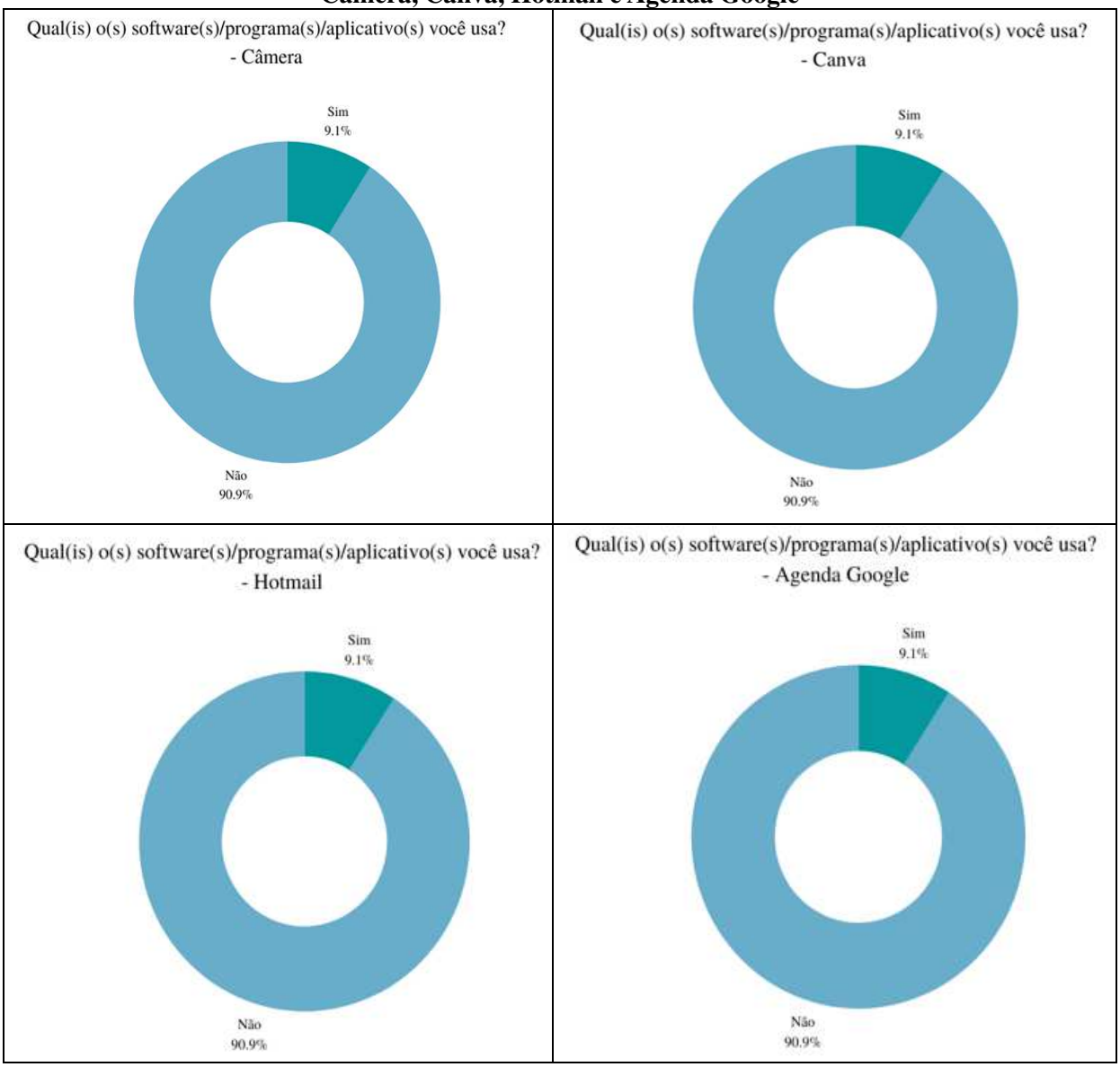
Gráfico 1 – Percentual de pessoal que utilizam algum software/programa /aplicativo não padrão da empresa



Mediante os dados recolhidos na primeira pergunta foram citados os softwares e aplicativos: Câmera do *smartphone*, Canva, Hotmail, Google Agenda, Instagram, *Whatsapp* Gmail.

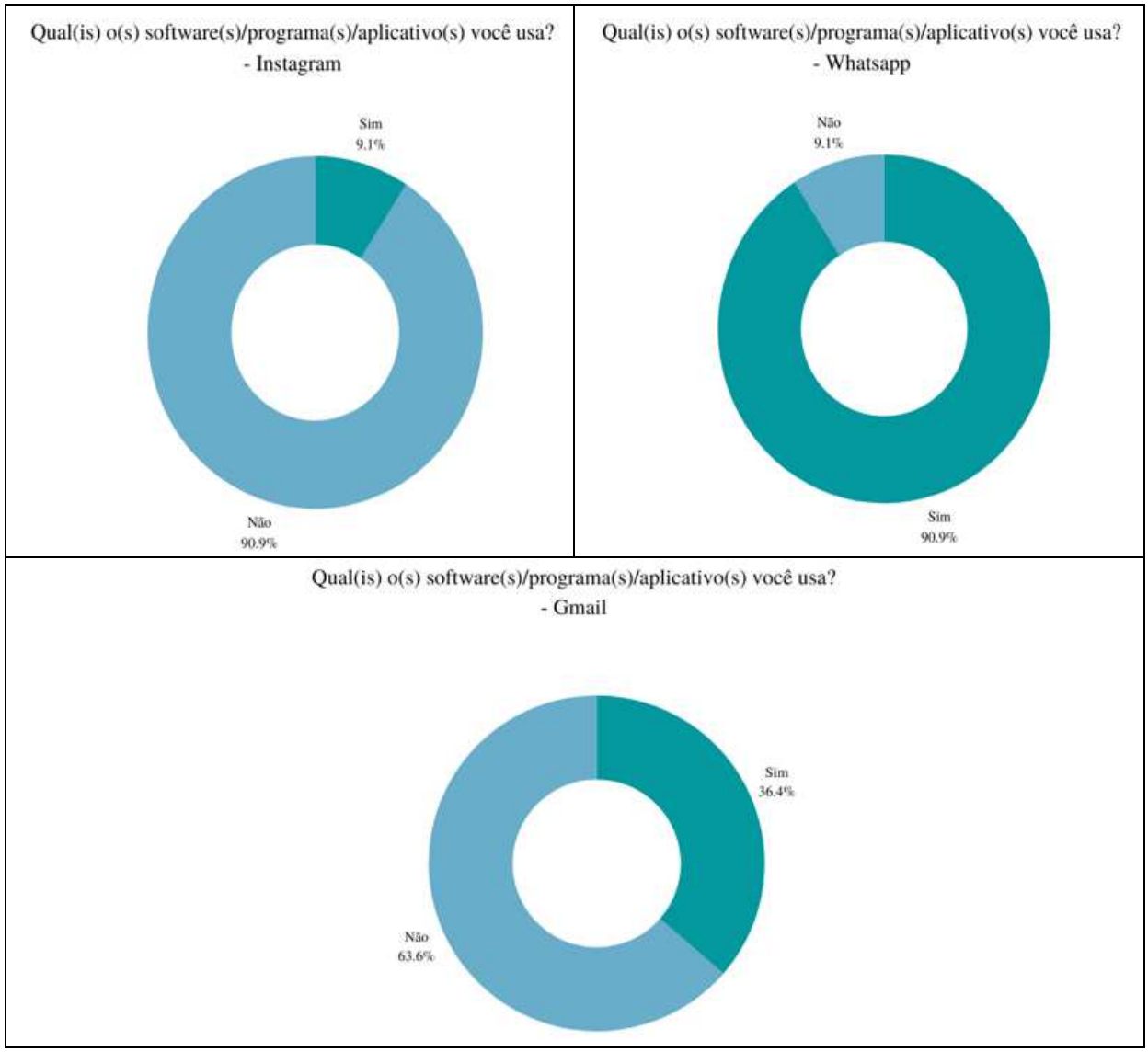
Com base no que foi mencionado pelos usuários na 1ª pergunta, foi perguntado a todos os entrevistados, em relação a cada software/programa/aplicativo sua utilização. Primeiramente, os resultados para os 4 primeiros são apresentados nos gráficos de 02 a 05, a seguir.

Gráficos 2, 3, 4 e 5 – Resultados da utilização de softwares/programas/aplicativos por usuários: Câmera, Canva, Hotmail e Agenda Google



Os resultados de utilização em relação aos softwares/programas/aplicativos sua utilização. Primeiramente, os resultados para os 4 primeiros são apresentados nos gráficos de 06 a 08, a seguir.

Gráficos 6 e 8 – Resultados da utilização de softwares/programas/aplicativos por usuários: Instagram, WhatsApp e Gmail

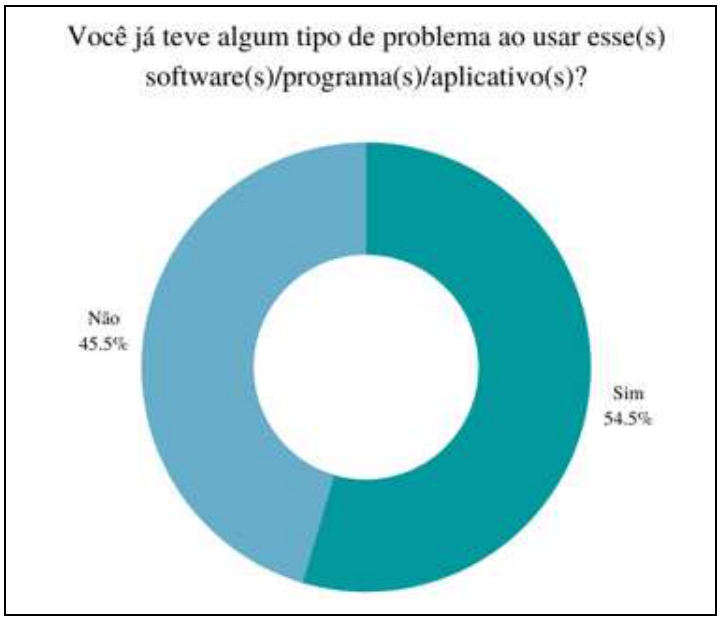


Na terceira pergunta, o aplicativo *Whatsapp* é usado por todos os entrevistados para envio e recebimento de arquivos como: Notas Fiscais, contratos, propostas, comprovantes de pagamento, pedidos de veículos ou peças etc.; já os aplicativos de e-mail (Gmail e Hotmail) são usados por 50% dos entrevistados, pois segundo alguns entrevistados o e-mail corporativo tem limite de tamanho para arquivos anexados; é importante mencionar que é utilizado e-mail pessoal para pois os entrevistados receberam os mesmos em seus dispositivos, reforçando o uso do e-mail pessoal para esse tipo de situação; os demais 50% alegam não usar aplicativos de e-mail pessoal. Apenas uma entrevistada informou que usa a Google Agenda para organizar suas tarefas e compromissos diários, mensais e anuais, também como saber o dia exato para ligar para clientes que estão em pendência. Por fim, uma entrevistada afirmou que usa a câmera do seu telefone para registrar fotos de veículos que precisam de atendimentos como manutenção e funilaria.

Seguindo com a quarta e última pergunta, 54.5% dos entrevistados alegam ter passado por problemas durante o uso desses softwares dentre os quais se pode citar: os aplicativos de e-mails e *Whatsapp* apresentaram arquivos corrompidos quando recebidos e é necessário pedir para que o remetente realize novamente o envio; e, o aplicativo do Gmail apresenta erro

no envio de mensagem se não for inserido o assunto na mensagem, cancelando assim o envio. Os demais 45.5% informaram que não tiveram nenhum tipo de problema com seus aplicativos. Conforme o Gráfico 9.

Gráfico 9 – Resultados da utilização de softwares/programas/aplicativos por usuários: Instagram, WhatsApp e Gmail



Cerca de 90% dos entrevistados são funcionários subordinados e não gestores, reforça-se que nos setores nos quais foram realizadas a entrevista, apenas uma pessoa era gestor (correspondendo a10%) da área de relacionamento da empresa, mas sem subordinado.

5. Conclusões

Mediante a observância dos dados e informações obtidos, constata-se que a amostragem dos entrevistados representa os funcionários que adotam persistentemente o *BYOD* e a *Shadow IT* sendo separados em duas vertentes: uma por livre e espontânea vontade onde os colaboradores usam dispositivos pessoais e softwares fora do controle da TI para executar suas tarefas de forma rápida, sem burocracias e permissões de administrador; a outra vertente é pela falta de recursos disponibilizado em favor dos funcionários para o *BYOD* e *Shadow IT*.

Quando mencionado que os recursos são limitados para o *BYOD,* afirma-se que a organização não provê 100% das necessidades dos funcionários, equipamentos corporativos antigos como telefone móvel sem a possibilidade de instalar o WhatsApp por exemplo dificulta muito a agilidade no momento das atividades, nesse caso muita das vezes o caminho mais fácil é pegar o telefone móvel pessoal para tal fim. Ressalta-se que o funcionário, no momento dessa ação, não tem a compreensão necessária a respeito da segurança dos dados presentes em um arquivo ou na transferência de um documento, via telefone móvel pessoal para os computadores corporativos.

Quando mencionado que os recursos são limitados para a *Shadow IT,* diz-se que a organização não provê 100% das necessidades dos funcionários e os softwares que necessitam de licença, ou algum tipo de compra, são deixados de lado, e buscam-se por opções

alternativas que reduzam os custos. Estas, muita das vezes, não suportam a execução das atividades, sendo limitadas por ser *Open Source*.

Em conversa com o supervisor de TI responsável pela organização em questão, para buscar saber como o departamento de TI tem se comportado mediante o cenário da empresa. Antes do resultado desta pesquisa, segundo esse supervisor, é realizada reunião diária de segunda-feira a sexta-feira para tratar casos referentes os equipamentos (hardware) caso esses estejam relacionados ao desempenho dos computadores de modo geral. Um detalhe muito importante e que chamou atenção foi sobre os programas que estão sendo instalados nos computadores como também sites de serviços pesquisados nos navegadores, com esse pressuposto o departamento de TI vem monitorando e controlando essas práticas que sinaliza o uso de *Shadow IT*. Porém veio uma dúvida, somente pela reunião é feito o controle de *Shadow IT*? O supervisor prontamente informou que não, além da análise superficial existe uma central que monitora toda atividade suspeita ou não suspeita para prevenir possíveis ataques cibernéticos mediante as vulnerabilidades deixadas pela *Shadow IT*, *"o FortiGate é o responsável por esse papel"*, disse ele, onde existe os recursos de segurança essenciais, antivírus, prevenção de intrusão, filtragem web, *antispam* e *traffic shaping*.

Destaca-se também, que para o supervisor, sobre a questão do uso de dispositivos pessoais pelos colaboradores dentro da organização e ele foi bem claro informando que todos os colaboradores no início de suas atividades recebem um telefone celular corporativo, porém é raro receber um que suporta os aplicativos que atendem as necessidades do colaborador para as tarefas da empresa, ficando assim uma lacuna na segurança da informação. Segundo comentado pelo supervisor durante a pesquisa de campo *"A intervenção do departamento de TI sobre essa questão é a conscientização sobre o uso dos dispositivos pessoais para as atividades de trabalho e que cabe a cada um manter a ética e disciplina com os arquivos e dados que se recebe"*.

De acordo com a análise dos resultados da pesquisa e informações recebidas através do supervisor de TI da organização as práticas de *BYOD* e *Shadow IT* estão sendo tratadas parcialmente, enquanto por um lado (*Shadow IT*) o cuidado é mais notável, por outro (*BYOD*), é insuficiente. Uma organização consegue coibir possíveis ataques ou falhas dentro de seus servidores e sistemas quando os dois lados da TI estão sendo tratados em igual teor, a saber, hardware e software.

6. Referências

Andrade, I. C. de M.; Pampanelli, G. A.; Cintra, S. P. V.; et al. 2020. "*BYOD*: Avanço tecnológico, modismo ou problema organizacional?" Em: XII Simpósio de Excelência em Gestão e Tecnologia (SEGeT). Disponível em: https://www.aedb.br/seget/arquivos/artigos16/352436.pdf. Acesso em: 15.11.2021.

Chiavenato, I. "Gestão de Pessoas: O novo papel dos recursos humanos nas organizações". 3ª edição. Elsevier: Rio de Janeiro, 2008.

Cisco. BYOD: uma perspectiva global aproveitando a inovação liderada pelo funcionário, 2012. Disponível em: https://www.cisco.com/c/dam/en_us/about/ac79. Acesso em: 05.07.2022.

Ferreira, K. "Implantação do Modelo de Mobilidade Corporativa (BYOD) na Indústria". CONTECSI 2019. Disponível em: https://www.tecsi.org/contecsi/index.php/contecsi/16CONTECSI/paper/view/6040/3472. Acesso em: 05.07.2021.

Gruman, G.. “The real force behind the Consumerization of IT”. Janeiro, 2012. Disponível em: https://www.infoworld.com/article/2614949/the-real-force-behind-the-consumerization-of-it.html. Acesso em: 03.11.2020.

Institute Training, Fortinet: “Network Security Associate 2”. Disponível em: https://training.fortinet.com/local/staticpage/view.php?page=nse_2**.** Acesso em: 01.07.2022.

Kalendae. “Shadow IT: o que é e quais os riscos relacionados?”. Setembro, 2019. Disponível em: https://kalendae.com.br/blog/o-que-e-shadow-it. Acesso em: 18.04.2021.

Kussama, L.Y. 2017. “Uma contribuição para avaliação do valor adicionado pela Shadow IT na organização pública brasileira”. Dissertação (Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos). São Paulo: CPS, 2017. 60f.

Monteiro Júnior, A. G. “As práticas de Shadow IT nas empresas”. Dissertação de Mestrado na PUC-SP. São Paulo, 2019. Disponível em: https://tede2.pucsp.br/handle/handle/21967. Acesso em: 01.11.2021.

Nativa. “Entenda as vantagens e desvantagens do BYOD”. Agosto, 2018. Disponível em: https://navita.com.br/blog/entenda-as-vantagens-e-desvantagens-do-byod. Acesso em: 04.03.2021.

Nakamura, E. T.; Geus. P. L. “Segurança de Rede em Ambientes Cooperativos”. Novatec. v. 1, p. 44-66, 2007.

Today, L. T.. “O que é Shadow IT e como ela pode impactar seus resultados”. Disponível em: https://techtoday.lenovo.com/br/pt/solutions/smb/o-que-e-shadow-it-e-como-ela-pode-impactar-seus-resultados. Acesso em: 04.03.2021.

NETO, Helson. BYOD & LGPD. LGPD Connect 2022, p. 1-6, Setembro, 2022. Disponível em: <https://www.linkedin.com/posts/anppd_artigo-byod-lgpd-activity-6976140826460499968-EEuw?utm_source=share&utm_medium=member_desktop>.