UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
CURSO DE ADMINISTRAÇÃO

RALDINEY FARIAS DA SILVA

GESTÃO DA NOVA TI SOB UMA PERSPECTIVA TÉCNICA E SOCIAL: UMA ANÁLISE DO USO DO BYOD NA UNIVERSIDADE FEDERAL DE CAMPINA GRANDE

CAMPINA GRANDE
2019

RALDINEY FARIAS DA SILVA

GESTÃO DA NOVA TI SOB UMA PERSPECTIVA TÉCNICA E SOCIAL: UMA ANÁLISE DO USO DO BYOD NA UNIVERSIDADE FEDERAL DE CAMPINA GRANDE

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Administração, da Universidade Federal de Campina Grande, em cumprimento parcial das exigências para obtenção do título de Bacharel em Administração.

Orientadora: Professora Dra. Petruska de Araújo Machado. Possui graduação em Tecnologia em Processamento de Dados pela Associação Paraibana de Processamento de Dados (2001), graduação em Administração pela Universidade Federal da Paraíba (2008), mestrado em Administração pela Universidade Federal da Paraíba (2011) e doutorado em Administração pela Universidade Federal do Rio Grande do Norte (2018) com doutorado sanduíche na Aston Business School da Aston University - Reino Unido (2017). Atua como Professora Visitante na Universidade Federal de Campina Grande no Curso de Pós-Graduação em Administração da Unidade Acadêmica de Administração e Contabilidade. Tem experiência na área de Administração e de TI, atuando principalmente nos seguintes temas: adoção e uso de tecnologia da informação, inovação de TI, TI Verde, tomada de decisão e comportamento organizacional.

CAMPINA GRANDE
2019

GESTÃO DA NOVA TI SOB UMA PERSPECTIVA TÉCNICA E SOCIAL: UMA ANÁLISE DO USO DO BYOD NA UNIVERSIDADE FEDERAL DE CAMPINA GRANDE

Raldiney Farias Da Silva[1]
Petruska de Araújo Machado[2]

RESUMO

As mudanças no gerenciamento da TI são decorrentes da evolução da tecnologia e da necessidade de melhorar as práticas das organizações. Neste estudo de caso, a nova TI é representada pelo uso de dispositivos móveis conhecido como fenômeno BYOD (*Bring your own device*). O objetivo desse estudo é analisar os fatores sociotécnicos associados ao uso do BYOD nas atividades de trabalho da UFCG à luz da abordagem sociotécnica. A identificação foi norteada pelas subdimensões (técnica e social) de Palvia et al., (2001). Este artigo oferece um estudo aplicado por discutir assuntos ainda difusos e escassos na literatura. Uma contribuição prática é que a compreensão das perspectivas técnicas e sociais que podem ajudar os gestores a entenderem e se adequarem às transformações e inovações tecnológicas como o uso do BYOD e que poderão ser implementadas por meio de técnicas de boas práticas de gestão.

Palavras-Chave: BYOD. Tecnologia. Inovação. Segurança

NEW IT MANAGEMENT UNDER A TECHNICAL AND SOCIAL PERSPECTIVE: AN ANALYSIS OF BYOD USE IN CAMPINA GRANDE FEDERAL UNIVERSITY

ABSTRACT

Changes in IT management stem from evolving technology and the need to improve organizations' practices. In this theoretical essay, the new IT is represented by the use of mobile devices known as the Bring your own device (BYOD) phenomenon. The aim of this study is to analyze the sociotechnical factors associated with the use of BYOD in UFCG work activities in light of the sociotechnical approach. The identification was guided by the sub-dimensions (technical and social) of Palvia et al., (2001). This article offers a theoretical contribution by discussing still diffuse and scarce subjects in the literature. A practical contribution is that understanding the technical and social perspectives that can help managers understand and adapt to technological transformations and innovations such as the use of BYOD and which can be implemented through good management practice techniques.

Keywords: BYOD. Technology. Innovation. Securit

[1] Raldiney Farias Da Silva, Graduando do Curso de Administração na Universidade Federal de Campina Grande. Email: ralfarias@hotmail.com

[2] Petruska de Araújo Machado, Possui doutorado em Administração pela Universidade Federal do Rio Grande do Norte (2018) . Atua como Professora Visitante na Universidade Federal de Campina Grande. Email: petruska.machado@ufcg.edu.br

1. INTRODUÇÃO –

Com a grande propagação de dispositivos móveis como celular, tablets e notebooks no cenário atual do mundo, as organizações estão cada vez mais preocupadas em como trabalhar da melhor forma essa questão no ambiente de trabalho. O fenômeno BYOD – bring your own device (traga seu próprio dispositivo), surge com ideia de reduzir custos de equipamentos, engajar e motivar o funcionário e dar praticidade na execução das funções, pois os mesmos estarão usando seus próprios dispositivos em suas atividades ao invés de dispositivos oferecidos pela organização. O BYOD é definido como uma ação de trazer o seu próprio dispositivo para o trabalho, conectando-os com a rede corporativa e usando para os negócios (LOOSE et al 2013).

Um dos principais desafios da implementação do BYOD é a questão da segurança, pois na maioria das vezes os dispositivos pessoais não são gerenciados pelo departamento de TI das organizações e correm o risco de serem o fator causador de possíveis invasões ao sistema, com possíveis vazamentos de dados (MORROW, 2012).

É importante a organização que pensa em implementar o BYOD planejar políticas de segurança visando a integridade dos seus dados juntamente com seus funcionários, pois os dispositivos dos mesmos podem ser a principal ameaça para o sistema interno, uma vez que podem ser facilmente infectados com arquivos maliciosos e demais tipos de vírus.

Uma questão que deverá ser levada em consideração em relação à segurança na aplicação BYOD é a privacidade, é preciso separar os dados da organização com os dados pessoais dos funcionários, para isso uma das muitas alternativas pode ser a computação em nuvem que nesse caso poderia ser utilizada com dois particionamentos, um para os dados da organização e outro para os dados pessoais do funcionário (MILLER, 2012).

O uso dessas tecnologias faz com que os funcionários se tornem a maior ameaça para a segurança da organização. Uma pesquisa realizada pela Forrester mostra que mais de 50% dos ataques a recursos dentro das organizações foram provocados por incidentes como: funcionários que acessam computadores de trabalho por meio de USB, funcionários que perdem laptop, tablets ou dispositivos de armazenamento com informações privadas da organização, funcionários que ignoram as políticas de segurança para levar trabalho para casa (FORCEPOINT, 2016). Todos esses incidentes podem ser potencializados pelos dispositivos de BYOD (Afreen, 2014).

Em particular, essas tecnologias mudam os processos e ferramentas de gerenciamento da TI, trazendo desafios para o trabalho dos profissionais de TI, provocando a perda de

controle sobre quem tem acesso as suas redes corporativas e exigindo novas habilidades e responsabilidades do departamento de TI (THOMSON, 2012). Para solucionar esses problemas é necessário realizar mudanças na forma como os recursos de TI devem ser gerenciados e adaptados para alinhar as necessidades organizacionais e individuais.

A definição para esse novo tipo de TI representa o que McKinsey&Company (2010) chama de tecnologias de transformação, ou seja, são aquelas que mudam a dinâmica da organização e que são demandadas pelos usuários e pelas unidades, para aumentar a flexibilidade e impulsionar a inovação. Exemplos da nova TI podem ser representados por aplicativos da Web, *cloud computing* e tecnologias provenientes do fenômeno BYOD (ex.: dispositivos privados como *smartphones*, *tablets*, *laptops*).

Devido a facilidade do uso e a expansão cada vez maior dos dispositivos móveis pessoais no cenário atual do mundo, essa pesquisa se justifica na perspectiva de entender os impactos que estão sendo causados com essa nova TI representada pelo uso do BYOD nas atribuições das atividades por parte dos funcionários e de como os mesmos estão reagindo a esse fenômeno.

Com isso, surgem as seguintes questões de pesquisa: 1) Quais os fatores sociais presentes na dinâmica de relacionamento entre indivíduos e nas suas atividades de trabalho a partir do uso do BYOD? 2) Quais fatores técnicos presentes na estrutura do trabalho e nos aspectos tecnológicos da organização a partir do uso do BYOD?

O objetivo desse estudo é analisar os fatores sociotécnicos associados ao uso do BYOD nas atividades de trabalho da UFCG à luz da abordagem sociotécnica.

A discussão sobre a gestão da nova TI em organizações foi norteada pelos aspectos técnicos e sociais do gerenciamento, baseada nos argumentos de Palvia *et al*., (2001) que sustentam que as mudanças que influenciam um ambiente organizacional tendem a proporcionar impactos técnicos e sociais que devem ser compreendidos e gerenciados para que não haja resistência.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. Aplicações da Nova TI: BRING YOUR OWN DEVICE

Diante da emergência da nova TI, os departamentos de TI depositam esforços para desenvolver um serviço padrão e de qualidade para oferecer aos seus clientes (usuários) (LOOSE et al., 2013). Freqüentemente, esses esforços visam reduzir custos e garantir o gerenciamento e a segurança da TI. Contudo, essa emergência parece comprometer o trabalho dos profissionais de TI por estar demandando novas formas de lidar com os recursos tecnológicos e humanos.

É verdade que o mundo dos dispositivos inteligentes e das tecnologias móveis são adotado não somente por usuários individuais, mas por um considerável número de organizações. Sendo assim, o BYOD abraçou novas perspectivas móveis no ambiente de trabalho (GEORGIADIS et al., 2013).

Seu conceito pode ser estendido dentro de um conjunto de serviços de BYOD que permite usuários escolher e usar os dispositivos que melhor atendem suas necessidades pessoais e de negócio. Nesta situação, a equipe de TI não consegue mais padronizar os dispositivos e os *softwares* utilizados no ambiente de trabalho (LOOSE et al, 2013).

O objetivo do fenômeno do BYOD é permitir que os usuários utilizem os seus próprios dispositivos para aumentar a eficiência e a flexibilidade no trabalho. Isso significa economia para a organização, porque reduz os gastos com fornecimento e gerenciamento de dispositivos (MORROW, 2012). Porém, o grande desafio é que os colaboradores passam a usar dispositivos que não são gerenciados pelo departamento de TI, dificultando o controle de acesso dos usuários aos recursos tecnológicos da organização, uma vez que o BYOD requer o gerenciamento de vários sofisticados dispositivos que mantém diferentes aplicações (DISTERER e KLEINER, 2013; MORROW, 2012).

Assim, organizações que desejam aproveitar as vantagens do BYOD devem estar preparadas para administrar todos os desafios relacionados à sua implantação, possibilitando assim colocar sistemas e práticas no ambiente corporativo de forma eficiente, garantindo serviços previsíveis, confiáveis, que não comprometam a integridade dos ativos da informação (CUNHA e CASTRO, 2014).

2.2. Segurança e privacidade no BYOD

Uma das preocupações das organizações com o uso do BYOD é a questão da segurança, pois os dispositivos na maioria das vezes não são gerenciados pelo departamento de TI, com isso estão mais susceptíveis e vulneráveis a possíveis vazamentos de dados e roubos de informações (MORROW, 2012).

Com os dispositivos pessoais, a organização tem um poder de controle muito fraco, com isso, fica totalmente dependente que os funcionários possuam boas práticas de segurança para garantir um bom funcionamento e assegurar que o acesso estará seguro via BYOD. Porém, não é sempre que os funcionários estarão dispostos a implementar as recomendações sugeridas, aumentando assim os riscos de violação e segurança (DHINGRA, 2016).

Os dispositivos BYOD requerem segurança adicional contra ameaças externas, cabe ao administrador do setor de TI da organização fazer o gerenciamento das medidas preventivas nos dispositivos para evitar qualquer problema que possa prejudicar os dados organizacionais. Sem essas medidas e ferramentas de segurança, as vantagens do uso do BYOD serão ofuscadas com os possíveis problemas que poderão surgir para a organização (HONG, 2016).

Um fator importante que não pode ser deixado de lado é a questão da privacidade, pois o uso do BYOD é diretamente ligado aos dispositivos pessoais com informações e arquivos privados dos usuários. Por isso, o fator da segurança é primordial para o bom funcionamento do BYOD, pois assegura a proteção de dados da organização e ao mesmo tempo assegura a confidencialidade dos dados privados dos usuários (MILLER, 2012).

Existe também a preocupação do funcionário não estar sendo espionado por seu superior, uma vez que as novas tecnologias podem permitir isso através de gps ou outros aplicativos de rastreio, podendo até ser usado em determinadas situações contra o próprio funcionário, por isso as políticas de uso do BYOD na organização deve ser claras para evitar possíveis invasões de privacidade (AFREEN, 2014).

2.4. Abordagem Sociotécnica

Neste artigo, a discussão de questões relacionadas ao gerenciamento da nova TI tem como norteadores os subsistemas da abordagem sociotécnica de Palvia *et al.* (2001), são eles: 1) técnico; e 2) social. O primeiro envolve as tarefas a serem realizadas e a tecnologia que

habilita essa realização; o último envolve os indivíduos responsáveis pela realização das tarefas e os trabalhos que devem ser coordenados.

Conforme Mumford (2006), a ênfase sociotécnica envolve: a tecnologia e sua associação com a estrutura de trabalho; e o sistema social sobre os grupos de indivíduos, coordenação, controle, delegação de responsabilidades. O objetivo do projeto sociotécnico é realizar a junção otimizada do sistema técnico e social. Contudo, este artigo não pretende realizar a associação entre os subsistemas sociotécnicos, mas utilizá-los para nortear a discussão do gerenciamento da nova TI.

2.4.1 Aspectos técnicos

Na tentativa de atender necessidades estratégicas de negócio, a difusão de novas tecnologias e as transformações nas estruturas organizacionais proporcionaram mudanças na forma como a TI executa as suas atividades e gerencia os recursos de TI. Dentre esses recursos, a infraestrutura de TI passou por significativa evolução que começa com uma estrutura centralizada até uma estrutura mais flexível e descentralizada. O quadro 1 mostra características da infraestrutura de TI e necessidades de gerenciamento ao longo das transformações tecnológicas.

Inicialmente, a arquitetura era baseada em *mainframes* que eram computadores de grande porte dedicados para processar grandes volumes de informação. Os mainframes tinham um custo muito alto e era preciso contratar profissionais altamente especializados para manter a arquitetura. A preocupação da TI era em como otimizar os recursos, deixando para segundo plano a flexibilidade do usuário (VERAS, 2012).

Após a era da arquitetura de *mainframe*, surgiu a arquitetura de rede cliente-servidor. Essa arquitetura ofereceu uma estrutura descentralizada e proporcionou a redução de custos para o departamento de TI, pois permitia o compartilhamento de recursos tecnológicos através das redes de computadores. Apesar dos custos mais baixos, o departamento de TI permaneceu com os custos de licenças de sistemas operacionais e de aplicações de softwares que eram gerenciados e mantidos pelo departamento de TI.

Quadro 1 - Evolução das tecnologias de infraestrutura

TECNOLOGIAS	Tecnologia	Economia	Modelo de Negócios
Mainframe	Centralizada	Otimizado para eficiência dos recursos devido o alto custo.	Altos custos com hardware e software
Cliente-servidor	Descentralizada	Otimizado para agilidade devido o baixo custo.	Licenças de sistemas operacionais e aplicações de softwares.
Cloud computing	Escalabilidade, comodidade e dispositivos	Eficiência e agilidade em busca de melhorar a magnitude.	Habilita a forma de como pagar, bem como, pagar apenas o que é usado.

Fonte: Adaptado de Harms e Yamartino (2010)

As novas demandas proporcionadas pela Internet e o desenvolvimento da tecnologia transformaram a arquitetura de TI com uma nova forma de oferecer serviços por meio da virtualização. A virtualização da tecnologia representa a abstração de recursos de computador (CPU, armazenamento, banco de dados, aplicações, etc), oferecendo uma plataforma com maior escalabilidade e compartilhamento de recursos (MATHER et al, 2009). É uma plataforma que fomenta o *cloud computing* (MATHER et al, 2009).

A tecnologia de *cloud computing* padroniza os recursos de TI e automatiza muitas tarefas de manutenção. Neste sentido, as plataformas de desenvolvimento e *desktops* virtuais e a centralização de *data centers* em provedores de serviços livraram os profissionais de TI das atividades operacionais. Com isso, a TI passa a terceirizar serviços, pagando apenas pelos serviços que utiliza. Além disso. em serviços de virtualização terceirizados, o departamento de TI não tem controle sobre a infraestrutura física, mas sobre as máquinas virtuais, armazenamento, aplicativos instalados, bem como um controle limitado dos recursos de rede (VERAS, 2012).

Essa limitação foi potencializada pelo fenômeno BYOD, uma vez que as tecnologias de virtualização e a popularidade dos dispositivos móveis estimularam o uso de dispositivos pessoais no ambiente de trabalho. Rapidamente organizações resolveram adotar práticas de BYOD em busca de flexibilidade (ex.: acesso a informações sem limite de tempo, lugar ou distância) e inovação (ex.: compartilhar ideias com colaboradores usando dispositivos moveis). Essas iniciativas proporcionaram considerável redução nos gastos de TI como: aquisição, suporte e manutenção de dispositivos tecnológicos. Porém, apesar da redução dos custos, profissionais de TI passaram a enfrentar dificuldades para gerenciar dispositivos não pertencentes e não gerenciáveis pela organização. O desafio está em como a TI pode gerenciar o uso de diferentes dispositivos pessoais utilizados para acessar informações e aplicativos da organização.

Neste contexto, emerge uma das maiores preocupações dos gerentes de TI relacionada com o gerenciamento de riscos e de segurança. Com a tendência do BYOD, os profissionais

de TI não conseguem implantar e controlar políticas de segurança, por exemplo, o uso de softwares de antivírus, tornando mais difícil a tarefa de identificar *malwares* nos dispositivos dos usuários (MORROW, 2012). Ainda, a TI sente dificuldade para controlar a escolha e a versão do *browser* instalados pelos usuários, uma vez que não conseguem gerenciar as informações armazenadas em caches, *password store* and histórico do *browser* (MORROW, 2012).

Para resolver problemas de ameaças de segurança, Disterer e Kleiner (2013) apresentam um conceito arquitetural de *desktop* virtual que usam as mesmas arquiteturas de soluções de virtualização (ex.: *Amazon WorkSpace*). O seu objetivo é isolar as aplicações de negócio do resto dos sistemas e aplicativos existentes nos dispositivos pessoais. A arquitetura possui serviços de restrição como, por exemplo, a indisponibilidade do usuário de armazenar dados da organização em seus dispositivos, bem como permite gerenciar e processar a interação do usuário com os serviços.

Apesar de todas as preocupações com questões de segurança, os resultados da pesquisa global de McKinsey de 2010 revelam que os executivos de outras áreas não estão preocupados com essas questões, porque acreditam que o *cloud computing*, por exemplo, pode proporcionar um valor substancial e que os riscos potenciais são gerenciáveis. Um fator relevante e que os executivos podem estar mais preocupados em como a nova TI irá se alinhar e dar suporte ao negócio da organização. Perguntas do tipo “Como as novas demandas organizacionais podem ser suportadas pela nova TI?” necessitam de respostas.

Outro aspecto a ser considerado é a questão da padronização de aplicativos e softwares que apóiam as tarefas. Apesar da tecnologia de virtualização facilitar a padronização de *softwares* e aplicativos, a difusão do fenômeno BYOD permitiu a autonomia dos usuários para instalar aplicativos e sistemas em seus dispositivos com a finalidade de acessar os dados corporativos. Por um lado, essa autonomia pode proporcionar inovação, por outro, pode dificultar o gerenciamento dos aplicativos que estão sendo usados no ambiente de trabalho, uma vez que o departamento de TI perde o controle e a responsabilidade sobre as tarefas de seleção, instalação e padronização dos aplicativos e ferramentas de trabalho.

2.4.2 Aspectos sociais

Os usuários de TI estão mais sofisticados devido à proliferação de TI e uma ampla gama de aplicações inovadoras. As novas aplicações (ex.: disponíveis na computação em nuvem) são relativamente simples para que até mesmo os usuários mais inexperientes possam usá-las (MCKINSEY&COMPANY, 2010). Os usuários estão mais conscientes da tecnologia

no ambiente de trabalho a passam a escolher o software e os dispositivos adequados para o seu trabalho (NIEHAVES e ORTBACH, 2013). Isso reflete em uma mudança no relacionamento entre o departamento de TI e os usuários da organização (NIEHAVES e ORTBACH, 2013).

Presumivelmente, se algo está conectado na rede da instituição é porque foi aprovado, configurado e instalado pelo departamento de TI, contudo, por ser mais fácil o acesso a programas e aplicativos, usuários começam a ficar menos dependentes do departamento de TI (GIDDENS e TRIPP, 2014). Isso tende a criar uma relativa liberdade em torno de TI corporativa (MCKINSEY&COMPANY, 2010). A vantagem dessa autonomia é que os usuários podem realizar a manutenção dos dispositivos sem o controle da TI (NIEHAVES e ORTBACH, 2013), reduzindo assim a responsabilidade da TI fornecer e manter os dispositivos na organização. Por outro lado, o setor de TI pode acabar perdendo o seu poder quando outros departamentos ou usuários começam a comprar e manter sua própria tecnologia (KOCH e CURRY, 2014).

Este contexto gera não apenas problemas técnicos de segurança, mas também problemas sociais. Porque, apesar de organizações utilizarem sistemas de gerenciamento de dispositivos móveis que permitam reforçar políticas de segurança em dispositivos móveis pessoais, a completa implementação dessas políticas de segurança limita a funcionalidade dos dispositivos, situação que pode não ser tolerada pelos usuários que usam os seus dispositivos pessoais para fins de negócios (LEBEK et al., 2013).

Sendo assim, as políticas devem ser mais sofisticadas para garantir que a rede seja bloqueada e que haja um controle sobre o uso desses dispositivos (MANSFILED-DEVINE, 2012). Para isso, os usuários devem fazer parte da definição dessas políticas, porque normalmente eles conhecem os dispositivos mais do que a equipe de TI. Uma provável solução seria trabalhar junto com o usuário ao invés de controlá-los. Thomson (2012) argumenta que os usuários esperam que os profissionais de TI e CIOs (*Chief Information Officers*) percebam que eles podem usar seus dispositivos, em qualquer tempo ou lugar, sem colocar a organização em risco. O valor dessa cooperação pode contribuir para um melhor gerenciamento do BYOD.

O fenômeno do BYOD faz emergir outra realidade não muito comum no ambiente de trabalho, Disterer e Kleiner (2013) chamam esta realidade de "inovação orientada pelo usuário" que significa a possibilidade do usuário conciliar sua vida profissional com a pessoal, proporcionando horas de trabalho mais flexíveis. Segundo o estudo anual da CISCO "*Connected World*" de 2011, profissionais mais jovens percebem pouca distância entre a vida

de trabalho e vida pessoal. Essa situação parece gerar um problema de desempenho e produtividade dos colaboradores devido a essa flexibilidade no horário de trabalho.

O desafio está em como a equipe de TI pode gerenciar o uso desses dispositivos fazendo com que os usuários utilizem os dispositivos para fins profissionais, tornando o trabalho mais produtivo. Para isso, é preciso que a TI compreenda porque os usuários desejam fazer uso de dispositivos pessoais na rede da organização, para enfim diferenciar pessoas que desejam usá-los no trabalho para acessar redes socais (ex.: *Facebook*) ou emails pessoais, daqueles que desejam usá-los para o trabalho (MANSFIELD-DEVINE, 2012).

Assim, conversar com os usuários e compreender suas necessidades podem ser o primeiro passo para melhor gerenciar os dispositivos pessoais.

Apesar disso, algumas pesquisas alegam que o BYOD aumenta a produtividade e a satisfação dos usuários porque os usuários ganham autonomia para escolher os dispositivos privados nos quais estão mais familiarizados. Uma entrevista realizada por Mansfiled-Devine (2012) revela que os usuários trabalham de forma mais produtiva quando usam os seus próprios dispositivos, mais do que quando usam dispositivos impostos pela organização. Porém, é importante que sejam realizadas pesquisas empíricas para investigar a influência do uso da nova TI sobre a produtividade dos usuários. (SCARFO, 2012; DISTERER e KLEINER, 2013)

3. METODOLOGIA

Essa pesquisa foi classificada como um estudo de caso descritivo, foi realizada uma abordagem qualitative. O método de coleta de dados foi a entrevista, roteiro anexo I, com perguntas abertas a funcionários da Universidade Federal de Campina Grande, à pesquisa foi realizada do dia 07/10/2019 ao dia 18/10/2019. A técnica de análise foi baseada em Saldaña (2009) usando mecanismos de codificação e categorização. As análises utilizadas na pesquisa foram com base na análise de cluster, nuvem de palavras e mapa de projetos. A pesquisa foi desenvolvida a partir da revisão da literatura, identificando aspectos sociais e técnicos do BYOD no contexto organizacional. O público alvo da pesquisa foi funcionários que estejam ligados diretamente ao uso de tecnologia da informação para realizar suas atribuições em seus locais de trabalho. O estudo de caso foi não probabilístico, através da técnica de bola de neve, onde os indivíduos participantes indicavam novos participantes do seu ciclo de amizade, foram entrevistados oito funcionários.

Tabela 1 – Data e duração das entrevistas

	Data	Duração
Entrevista 1	07/10/2019	17:00 minutos
Entrevista 2	15/10/2019	20:00 minutos
Entrevista 3	15/10/2019	15:00 Minutos
Entrevista 4	15/10/2019	13:00 Minutos
Entrevista 5	16/10/2019	23:00 minutos
Entrevista 6	16/10/2019	21:00 Minutos
Entrevista 7	17/10/2019	19:00 Minutos
Entrevista 8	18/10/2019	25:00 Minutos

As entrevistas foram realizadas após consentimento do indivíduo de pesquisa após assinatura do termo livre e esclarecido com permissão para gravação. O autor comprometeu-se em não identificar os sujeitos pesquisados.

As transcrições das gravações ocorreram por meio do software NVivo 12 Plus. O NVivo é um software que auxilia a encontrar, analisar e organizar informações em dados qualitativos. (QSRINTERNATIONAL, 2019)

Para a medida de similaridade/distância foi usada a análise de cluster, que utiliza o coeficiente de correlação de Pearson, onde o NVivo 12 Plus fornece automaticamente seu cálculo. Com essa medida é avaliada a intensidade entre duas variáveis (x e y), onde os falores ficam entre –I e I. o Cálculo de Pearson é encontrado pela equação. (RAFFA *et al*., 2017)

Foram criadas categorias e sub categoria visando a organização dos dados coletados, são elas: Categoria: Estrutura; subcategorias (Permissão, Suporte do TI); Categoria: Pessoas; subcategorias (Autonomia, Benefícios, Fatores que podem comprometer o desempenho, Produtividade e Satisfação); Categoria: Tarefas; subcategorias (Desempenho, Desvantagens e Restrição); Categoria: Tecnologia; subcategorias (Precauções e Segurança).

3.1 Aplicação das Técnicas de Análise dos Dados

A análise dos dados foi realizada com o apoio do software QSR NVivo, utilizando mecanismos de codificação a partir da categorização do conteúdo do texto. A etapa de codificação seguiu dois ciclos. No primeiro ciclo da codificação, foi utilizado o método de codificação descritiva, resultando em 410 códigos descritivos. No segundo ciclo, utilizou-se a codificação por padrão a fim de revisar os códigos e identificar redundâncias, padronizar rótulos e enxugar a estrutura do modelo de codificação, resultando na redução de 51 códigos e um total de 359 códigos válidos (SALDAÑA, 2009).

O Quadro 1 mostra a quantidade de codificação em cada ciclo para cada categoria.

Tabela 2 - Quantidade de Códigos

Categoria	**Quantidade códigos – 1º Ciclo**	**Quantidade códigos - 2º Ciclo**
Social-Pessoas	99	81
Autonomia	8	8
Benefícios	18	16
Fatores que podem comprometer o desempenho	13	13
Produtividade	13	12
Satisfação	8	8
Social-Estrutura	36	25
Permissão	8	8
Suporte do TI	7	7
Técnico-Tecnologia	44	41
Precauções	15	14
Segurança	9	9
Técnico-Tarefas	82	68
Desempenho	18	18
Desvantagens	25	24
Restrição	7	7
TOTAL	**410**	**359**

O esquema de codificação seguiu um fluxo simples (Figura 2), tendo como ponto de partida a abordagem sociotécnica, a fim de orientar o processo de codificação dos dados. Os temas ou conceitos são os construtos mais abstratos e de mais alto nível relacionados com o desenvolvimento da teoria, representado por: mudanças no gerenciamento do BYOD (SALDAÑA, 2009, pg. 12).

A categorização foi baseada nas categorias identificadas na revisão da literatura e pré-definidas no modelo de pesquisa, são elas: pessoas, estrutura, tecnologia e tarefas. As subcategorias também emergiram da revisão da literatura. Os códigos são os dados que recebem um rótulo com significados que estão relacionados com as entrevistas (SALDAÑA, 2009). Os códigos foram criados a partir da análise de conteúdo nos artigos incluídos. As ferramentas utilizadas nas análises foram: O software QSR NVivo versão 12 Plus.

4. RESULTADOS E DISCUSSÃO

4.1 Descrição da amostra

Tabela 3 – Dados demográficos

	CARGO	IDADE	TEMPO DE TRABALHO	NÍVEL ESCOLAR	GÊNERO
Entrevistado 1	Secretária Executiva	31 anos	2 anos e 6 meses	Mestranda	Feminino
Entrevistado 2	Secretária Executiva	38 anos	9 anos	Mestrado	Feminino
Entrevistado 3	Assistente Administrativo	36 anos	6 anos	Superior Completo	Masculino
Entrevistado 4	Assistente administrativo	41 anos	10 anos	Superior Completo	Feminino
Entrevistado 5	Assistente Administrativo	57 anos	7 anos	Superior Completo	Feminino
Entrevistado 6	Secretária Executiva	27 anos	4 anos	Mestrado	Feminino
Entrevistado 7	Assistente administrativo	29 anos	2 anos	Superior Completo	Feminino
Entrevistado 8	Secretário Executivo	28 anos	4 anos	Mestrando	Masculino

Dos oito entrevistados, seis foram do sexo feminino e dois do sexo masculino, quatro possuem o cargo de secretaria e quatro possuem o cargo de assistente administrativo. Quatro dos entrevistados possuem de 28 a 32 anos, já os outros quatros possuem idade acima dos 33 anos, os oito possuem nível superior, dois possuem mestrado e dois estão cursando o mestrado.

4.2. Análise do mapa de Cluster

A análise de cluster consiste em uma técnica exploratória que permite visualizar os padrões no projeto, agrupando fontes ou nós, as palavras que aparecem juntas possuem uma forte semelhança, diferente das que aparecem separadas, os diagramas de análise de cluster fornecem uma representação gráfica, facilitando a visualização de semelhanças e diferenças. Com a análise de cluster também é possível verificar o nível de correlação, como mostra a tabela 4, o cálculo de Pearson é encontrado na fórmula mostrada na figura 1.

Figura 1 - Cálculo de Pearson

$$\rho = \frac{\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i-\bar{x})^2}\cdot\sqrt{\sum_{i=1}^{n}(y_i-\bar{y})^2}} = \frac{cov\,(X,Y)}{\sqrt{var(X)\cdot var(Y)}}$$

Fonte: (RAFFA et al., 2017,p. 25)

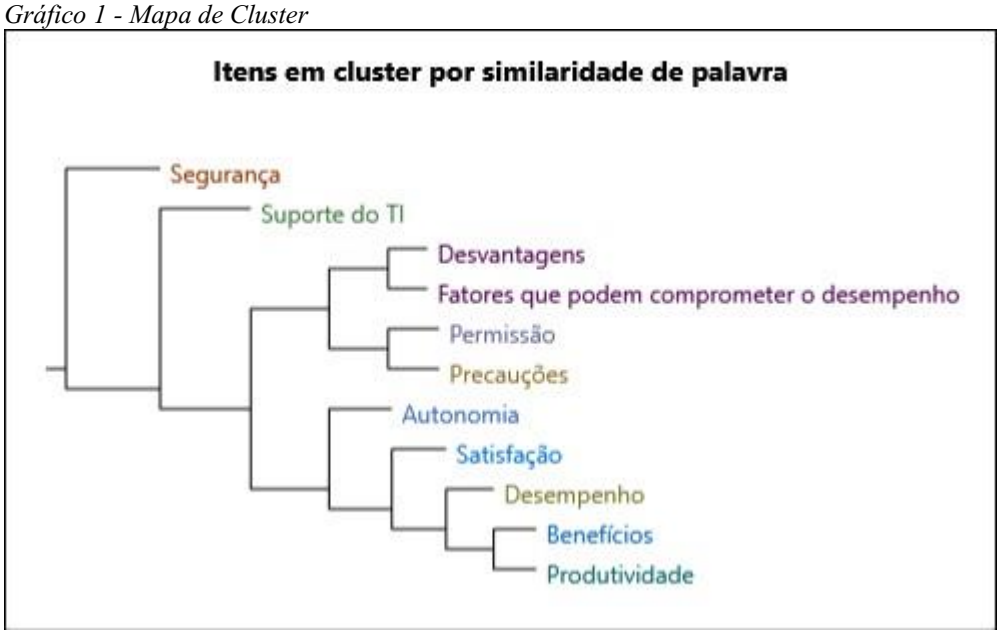
Interpretação do Coeficiente de Correlação de Pearson

Tabela 4 - Escala de Pearson

Escala de Pearson	Interpretação
0,00 a 0,19	Uma correlação bem fraca
0,20 a 0,39	Uma correlação fraca
0,40 a 0,69	Uma correlação moderada
0,70 a 0,89	Uma correlação forte
0,90 a I,00	Uma correlação muito forte

Fonte: Adaptado de Cramer e Howitt (2004, p. 38-40)

Gráfico 1 - Mapa de Cluster



Fonte: Extraído do software NVivo 12 Plus (2019)

Verificando o diagrama de Cluster Gráfico 1 relativo as subcategorias, percebe-se que a uma forte correlação entre Benefícios e Produtividade, isso acontece porque o indivíduo com os benefícios alcançados com o uso do BYOD tende a se tornar mais produtivo em seu ambiente de trabalho, a correspondência foi de (ρ=0,77).

Os clusters Desvantagens e Fatores que Podem Comprometer o Desempenho, também possuem grande proximidade, também merecendo destaque, a correlação é (ρ=0,80), a maior dessa análise, isso acontece, pois as desvantagens que os entrevistados afirmaram no uso dessa nova tecnologia são capazes de afetar e comprometer diretamente o desempenho nas suas funções de trabalho, por isso a organização deve estar preparada para tentar minimizar essas desvantagens para que o desempenho do funcionário não caia e sua produtividade seja afetada (CUNHA e CASTRO, 2014).

Com relação aos clusters Segurança e Suporte do TI, é notável uma maior distância dos demais, pois tiveram um dos menores graus de correlação com (ρ=0,27), devido à maioria dos entrevistados em suas respostas, afirmaram que nunca solicitaram o suporte do departamento de TI da organização sobre dúvida ou problema usando os dispositivos BYOD em suas tarefas, já em relação a segurança a maioria respondeu que toma apenas as precauções básicas, como exemplo, a instalação de antivírus em seus dispositivos.

4.3 Nuvem de Palavras

Durante a análise dos dados, também foi utilizado a nuvem de palavras, recurso do NVivo 12 Plus que mostra e permite a consulta das palavras com maior frequência dentro dos dados coletados.

Figura 2 - Nuvem de Palavras

Fonte: Extraído do software NVivo 12 Plus (2019)

Pelo método de nuvem de palavras é possível observar que as palavras que obtiveram maior frequência foram: Computador, Celular, Dispositivos, pois são consideradas primordiais para o uso do BYOD. A maioria das pessoas entrevistadas afirmaram que os dispositivos pessoais mais usados foram o computador e o celular, o uso se faz presente tanto no ambiente de trabalho como em suas próprias casas para resolver tarefas pendentes do trabalho que restaram do dia anterior ou até mesmo para resolver pendências, que aparecem esporadicamente nos finais de semana. As pessoas estão cada vez mais comprando dispositivos móveis avançados e utilizando aplicativos para facilitar as tarefas em seus cotidianos, com isso é natural que esses dispositivos sejam levados para o ambiente de trabalho e façam parte das atividades diárias de trabalho. (BRADLEY *et al*.2012)

Outras palavras que são destaque na figura 2 são: Desempenho, Praticidade e Agilidade. Essas três palavras estão interligadas pois fazem parte das vantagens do uso do BYOD relatadas pelos entrevistados, muitos afirmaram que depois da implantação do SEI

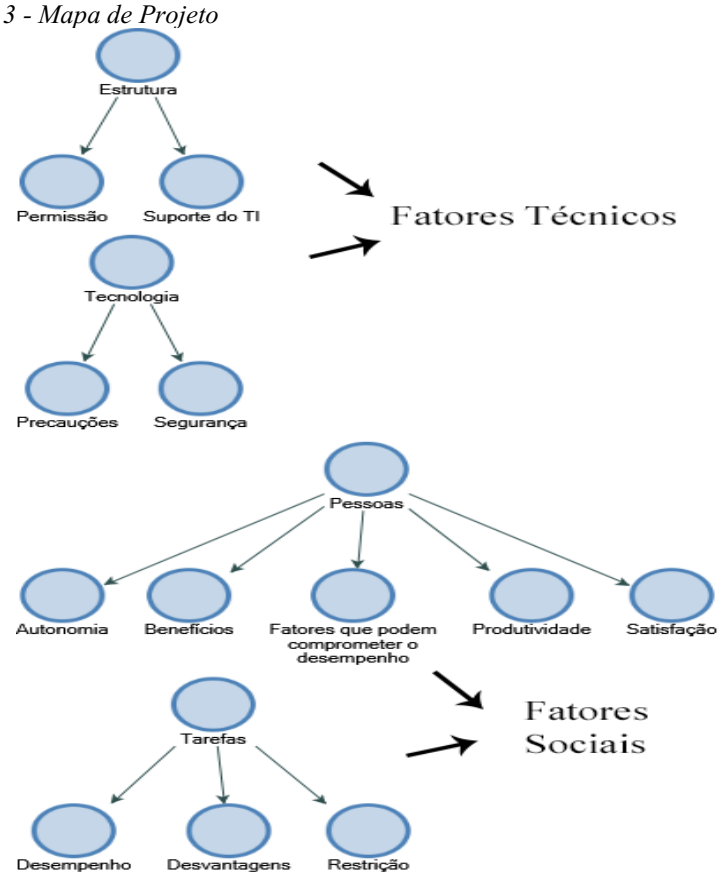
(Sistema Eletrônico de Informações) na Universidade Federal de Campina Grande, a resolução de processos melhorou muito, processos que poderiam demorar dias, hoje podem demorar minutos para serem despachados, com isso percebe-se que a gestão dessas novas tecnologias da informação tendem a se tornar cada vez mais importante nas tarefas dos funcionários.

A privacidade, que também está na nuvem de palavras, foi uma das questões que os funcionários relataram como desvantagens do uso do BYOD, alguns deles afirmaram que tem receio de acontecer algo com seus dados pessoais, outros afirmaram que temiam acontecer algo no sistema da organização e eles serem responsabilizados por isso. De acordo com Symantec's 2011 'Internet, mais da metade das ameaças do sistema operacional android, coletam dados ou rastreiam os dispositivos do usuário (MORROW, 2012).

4.4 Mapa do Projeto

O mapa de projeto identifica de maneira clara e objetiva as categorias e suas respectivas subcategorias ligadas por conectores, facilitando a visualização e o entendimento.

Figura 3 - Mapa de Projeto



Fonte: Extraído do software NVivo 12 Plus (2019)

4.4.1 Estrutura – Permissão

A maioria dos entrevistados responderam que desconhecem uma permissão oficial para acessar o sistema da instituição via dispositivos BYOD, porém também comentaram que desconhecem qualquer proibição. Segundo Harms e Yamartino (2010), Uma política de tecnologia descentralizada com aspectos de escalabilidade e comodidade agrega valor pois o indivíduo é livre para acessar os dados da organização e fazer o acesso ao seu sistema.

4.4.2 Estrurura – Suporte do TI

Foi identificado que a grande maioria dos entrevistados nunca solicitou suporte ao departamento de TI para seus dispositivos BYOD, alguns responderam que preferem pedir ajuda para uma pessoa de fora.

4.4.3 Tecnologia – Precauções:

As precauções mais citadas dos entrevistados foram não salvar a senha de acesso ao sistema da instituição nos dispositivos pessoais, não compartilhar com outros dispositivos o Token, o acesso via BYOD somente a sites confiáveis, o acesso a e-mails apenas da lista de contatos ou e-mails oficiais da instituição. Dhingra (2016), afirma que uma possível solução pode ser redes privadas virtuais, pois cria um canal seguro e garante proteção aos dados, podendo ser dividida em duas partes, uma parte para o acesso aos dados da empresa e uma parte para os dados pessoais.

4.4.4 Tecnologia – Segurança

Foi identificado a preocupação da instalação de programas antivírus, antispywares e antimalwares, necessitando de sempre estar com esses programas atualizados, porém a maioria dos entrevistados relataram que não tomam medidas de segurança no seu celular, com o argumento de que possíveis aplicativos antivírus tendem a deixar o celular mais lento, já nos notebooks a proteção é básica com programa de antivírus gratuitos. Para Morrow (2012), evitar que os dispositivos móveis sejam invadidos, e os dados sejam violados, a organização necessita tomar medidas proativas para que os dispositivos possam possuir controles de segurança adequados, com essas medidas a organização diminui os riscos de problemas com o uso do BYOD.

4.4.5 Pessoas – Autonomia

De modo unânime, os entrevistados relaram que possuem total autonomia para instalar e desinstalar o aplicativo que quiserem em seus dispositivos BYOD, sem nenhum tipo de restrição. Os malwares criados para dispositivos móveis são uma ameaça que vem crescendo cada vez mais, principalmente no android que pode ser uma plataforma aberta, com isso o cuidado para instalar aplicativos deve ser redobrado para evitar possíveis espiões nos dispositivos (MORROW, 2012).

4.4.6 Pessoas – Benefícios

Foi percebido nessa entrevista que o BYOD tráz muitos benefícios, entre eles estão a praticidade de resolver questões que antes eram burocráticas, flexibilidade para acessar o sistema de qualquer lugar que tenha internet, agilidade e mobilidade. Também pode motivar o funcionário a desempenhar sua função da melhor forma possível, fazendo com que o mesmo se torne mais produtivo para organização, também pode reduzir os custos, uma vez que o funcionário estará trabalhando com seu próprio dispositivo (SCARFO, 2012; DISTERER e KLEINER, 2013).

4.4.7 Pessoas - Fatores que Podem Comprometer o Desempenho

Foi identificado com entrevistados que as redes sociais são a principal causa que podem afetar o desempenho negativamente, pois a maioria revelou que perde o foco e a atenção do trabalho, depois vem à segurança da informação, onde alguns responderam que não acham seguro os dados pessoais acessando o sistema da organização via BYOD.

4.4.8 Pessoas – Produtividade:

Uma das maiores virtudes do uso do BYOD , não foi unânime, a maior parte dos entrevistados responderam que são mais produtivos usando os dispositivos pessoais para realizar suas tarefas, outros afirmaram que preferem os dispositivos fornecidos pela instituição, pois temem serem incomodados fora do horário e local de trabalho.

4.4.9 Pessoas – Satisfação

As vantagens do uso do BYOD são os principais fatores que trazem satisfação para os funcionários, foi assim que os entrevistados responderam, afirmaram que no aspecto geral, são satisfeitos com a agilidade e praticidade de como se resolve as coisas.

4.4.10 Tarefas – Desempenho

De acordo com os entrevistados, o uso do BYOD melhora o desempenho das suas atividades, desde que não ultrapasse os limites de privacidade, pois alguns funcionários revelaram que recebem e-mails e mensagens relacionadas ao trabalho fora da hora e do local de trabalho e rotularam essas práticas como invasivas. Raths (2012), afirma que o usuário se sente mais confortável usando seu dispositivo, pois já está familiarizado com o dispositivo.

4.4.11 Tarefas – Desvantagens

Dentro das desvantagens elencadas pelos entrevistados, as que mais se destacaram foi, as redes sociais, que podem atrapalhar a execução das atividades no tempo hábil, a privacidade, pois a organização poderá querer instalar programas nos dispositivos pessoais, até que ponto vai a relação pessoal/profissional e a segurança dos dados.

4.4.12 Tarefas – Restrição

Foi percebido com os entrevistados que a instituição não possui restrição quanto ao acesso via BYOD, Pois o acesso é totalmente liberado, caso haja alguma restrição, os funcionários afirmaram que desconhecem.

5. CONCLUSÃO

O objetivo desse estudo foi analisar os fatores sociotécnicos associados ao uso do BYOD nas atividades de trabalho da UFCG à luz da abordagem sociotécnica.

Sem dúvidas, as novas tecnologias estão mudando a forma de como as tarefas e atribuições estão sendo executadas nas organizações, com o intuito de facilitar, dar praticidade, reduzir custos e ainda motivar os funcionários, surge o fenômeno BYOD. Com isso veremos essa nova forma de encarar as tarefas de trabalho crescer cada vez mais, pois as organizações estão percebendo a melhora no rendimento de seus funcionários após a implantação dessa nova ferramenta da TI, com um processo de segurança bem estruturado e políticas claras de privacidade, as organizações estão aptas a desfrutarem das vantagens e benefícios que esse fenômeno pode trazer, fazendo assim que sua produtividade e competitividade aumentem no mercado.

Os fatores sociais (pessoas e tarefas) presentes foram, Pessoas com as subcategorias, Autonomia, onde o funcionário tem total liberdade para instalar aplicativos em seus dispositivos, Benefícios, sendo eles a praticidade para resolver suas atividades de trabalho, flexibilidade para poder acessar o sistema a hora e o local que quiser, agilidade na resolução dos processos e facilidade com o uso do seu próprio dispositivo. Produtividade, através da facilidade do uso do seu próprio dispositivo, quando o funcionário tem liberdade para escolher o próprio dispositivo, usar a tecnologia em nuvem e trabalhar no local desejado se torna mais produtivos. (SCARFO, 2012; DISTERER e KLEINER, 2013)

Satisfação, segundo Bradley (2018), quando os funcionários escolhem usar seus próprios dispositivos ficam mais satisfeitos no trabalho, além de melhorar seu desempenho.

As desvantagens ficam por conta da questão da privacidade e da segurança da informação, porém cabe a organização oferecer um bom e seguro sistema para desfrutar das vantagens do BYOD (BRADLEY *et al*.2012).

Os fatores técnicos (estrutura e tecnologia) presentes foram uma estrutura descentralizada onde os funcionários possuem acesso ao sistema da organização de qualquer lugar com qualquer dispositivo bastando apenas uma conexão com a internet, permitindo assim a expansão e adesão de novas tecnologias como o BYOD. A segurança adotada nos dispositivos pessoais dos funcionários para fazer o uso do BYOD é de extrema importância, os antivírus em seus dispositivos pessoais devem estar sempre atualizados e as precauções de para não entrar em qualquer site nem abrir qualquer e-mail devem ser essenciais, evitando assim, possíveis arquivos espiões. Os funcionários tem total permissão para acessar o sistema da instituição de qualquer dispositivo, ponto considerado positivo, pois descentraliza e desburocratiza o acesso ao sistema.

Esta pesquisa tem implicações acadêmicas e práticas. A implicação acadêmica é a tentativa de contribuir com a literatura com assuntos específicos da área de gerenciamento da nova TI com o enfoque no fenômeno BYOD. A implicação prática é que a compreensão das perspectivas técnicas e sociais que podem ajudar gestores a utilizar dispositivos pessoais para trazer maior praticidade, agilidade flexibilidade com segurança nas atividades de trabalho, podendo assim estar aprimorando o desempenho da organizacional.

A limitação da pesquisa foi à dificuldade de encontrar publicações na área de TI que abordassem o tema BYOD de forma mais estruturada, objetiva e focada em organizações públicas, comprometendo assim a elaboração de uma discussão com maior profundidade.

Para pesquisas futuras sugere-se uma pesquisa exploratória para investigar como o departamento de TI da Universidade Federal de Campina Grande está lhe dando com essas

novas tecnologias. Além disso, investigar como a adoção de práticas de BYOD impacta na segurança e privacidade tanto no sistema da organização como nos dispositivos pessoais dos usuários.

REFERÊNCIAS

Afreen, R. (2014). Bring your own device (BYOD) in higher education: opportunities and challenges. International Journal of Emerging Trends & Technology in Computer Science, Vol. 3, Issue 1, p. 233-236.

ANWAR, Z.; KHAN, W. A. Guess who is listening in to the board meeting: on the use of mobile device applications as roving spy bugs. Journal Security and Communication Networks, 8(16), p. 2813-2825, 2015.

BRADLEY, Joseph et al. BYOD: una perspectiva global. Horizons Cisco IBSG. Recuperado de< www. cisco. com>(consultado el 30 de enero de 2018), 2012.

CRAMER, Duncan; HOWITT, Dennis Laurence. The Sage dictionary of statistics: a practical resource for students in the social sciences. Sage, 2004.

CISCO. Connected world technology final report. 2011. http://www.cisco.com/c/en/us/solutions/enterprise/connected-world-technology-report/index.html. Acessado em: 29/12/2014

CUNHA, I. K. B.; CASTRO, R.C.C. Gestão da Segurança da Informação em ambientes BYOD: um mecanismo de apoio baseado nas boas práticas ITIL. Anais do EATI - Encontro Anual de Tecnologia da Informação e Semana Acadêmica de Tecnologia da Informação. Ano 4 n. 1, pp. 32 -39, 2014.

DHINGRA, Madhavi. Legal issues in secure implementation of bring your own device (BYOD). Procedia Computer Science, v. 78, p. 179-184, 2016.

DISTERER, G.; KLEINER, C. BYOD bring your own device. Procedia Technology, vol. 9, pp. 43-53, 2013.

FORCEPOINT. Global Threat Report. Acessado em 05/08/2016 https://www.forcepoint.com/, 2016.

GEORGIADIS, C.; STIAKAKIS, E.; ANDRONOUDI, A. The significance of mobile security breaches in terms of their economic impact on users. International Conference on Mobile Business, Page 7, 2014.

GIDDENS, L; TRIPP, J. It's my tool, I know how to use it: a theory of the impact of BYOD on device competence and job satisfaction. Twentieth Americas Conference on Information Systems, Savannah, 2014.

GLADYNG, C. BYOD: Can it Harm Your Business. In KESTLE, R.; SELF, R. IS practices for SME success series: the role of IS assurance & security management, 1º Ed., 2013.

HARMS, Rolf; YAMARTINO, Michael. The economics of the cloud. Microsoft whitepaper, Microsoft Corporation, 2010.

HARRIS, M.A.; PATTEN, K.; REGAN, E. The need for BYOD mobile device security awareness and training. Proceedings of the Nineteenth Americas Conference on Information Systems, Chicago, Illinois, August, pp. 15-17, 2013.

HONG, Sungmin et al. Towards SDN-Defined Programmable BYOD (Bring Your Own Device) Security. In: **NDSS**. 2016.

HSU, L. W-H. Governance Model of Cloud Computing Service. Special Report on Research & Innovation, n. 12, pp. 6-7, 2013.

JARAMILLO, D.; KATZ, N.; BODIN, B. et al. Cooperative solutions for Bring Your Own Device (BYOD). Vol. 57, n. 5, 2013.

JOHNSON, K. Meet BYOD challenges. SANS Mobility/BYOD Security Survey, March 2012.

KOCH, H.; CURRY, P. IT consumerization's impact on enterprise IT. Twentieth Americas Conference on Information Systems, Savannah, 2014.

LEBEK, B.; DEGIRMENCI, K.; BREITNER, M. H. Investigating the influence of security, privacy, and legal concerns on employees' intention to use BYOD mobile devices. Proceedings of the Nineteenth Americas Conference on Information Systems, Chicago, Illinois, August, pp. 15-17, 2013.

LOOSE, M.; WEEGER, A.; GEWALD, H. BYOD – The next big thing in recruiting? Examining the determinants of BYOD service adoption behavior from the perspective of future employees. Proceedings of the Nineteenth Americas Conference on Information Systems, pp. 15-17, August, 2013.

MAGALHÃES, I. L.; PINHEIRO, W. B. Gerenciamento de serviços de TI na Prática: uma abordagem com base na ITIL. São Paulo: Novatec, 2007.

MANSFIELD-DEVINE, S. Interview: BYOD and the enterprise network. Computer Fraud & Security, vol. 2012, n. 4, pp. 14-17, 2012.

MATHER, T.; KUMARASWAMY, S.; LATIF, S. Cloud Security and Privacy. 1ª Edition, O'Reilly Media: United States of America, 2009.

MCKINSEY&COMPANY. Como TI está gerenciando as novas demandas. Resultados da Pesquisa Global da McKinsey, 2010.

MILLER, Keith W.; VOAS, Jeffrey; HURLBURT, George F. BYOD: Security and privacy considerations. It Professional, v. 14, n. 5, p. 53-55, 2012.

MORROW, B. BYOD security challenges: control and protect your most sensitive data. Quarri Technologies: Network Security, 2012.

NIEHAVES, B.; KÖFFER, S.; ORTBACH, K. The effect of private IT use on work performance – towards an IT consumerization theory. 11th International Conference on Wirtschaftsinformati, Leipzig, Germany, 2013.

RAFFA, Claudia; MALIK, Ana Maria; PINOCHET, Luis Hernan Contreras. ANÁLISE DAS VARIÁVEIS DO AMBIENTE INTERNO NO GERENCIAMENTO DE LEITOS EM ORGANIZAÇÕES HOSPITALARES PRIVADAS: APLICAÇÃO DO SOFTWARE NVIVO. RAHIS, v. 14, n. 4, 2017.

RAGHU, I. Network Management and Security Challenges faced by organizations adopting BYOD. 5th International Conference on Security of Information and Networks (SIN), pp. 25-27, India, 2012.

RATHS, David. Are you ready for BYOD?. The Journal, v. 39, n. 4, p. 28-32, 2012.

OLIVEIRA, T.; THOMAS, M.; ESPADANAL, M. Assessing the determinants of cloud computing adoption: an analysis of the manufatucturing and services sectors. Information & Management, vol. 51, pp. 497-510, 2014.

PALVIA, S. C.; SHARMA, R. S.; CONRATH, D. W. A socio-technical framework for quality assessment of computer information systems. Industrial Management & Data Systems, vol. 101, n. 5, pp. 237-251, 2001.

SALDAÑA, J. The coding manual for qualitative researchers. Sage: London, 2009.

SCARFO, A. New security perspectives around BYOD. 7th International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA). Victoria, Canadá, pp. 12-14, 2012.

THOMSON, Gordon. BYOD: enabling the chaos. Network Security, v. 2012, n. 2, pp. 5-8, 2012.

VERAS, M. Cloud computing: nova arquitetura da TI. Rio de Janeiro: Brasport, 2012.

ANEXO I

Roteiro de entrevista

1) Comente sobre a permissão dada pela gestão da instituição ou pelo departamento de TI para usar os dispositivos pessoais para realização das suas atividades (por exemplo, uso de recursos tecnológicos como sistemas e acesso à dados da instituição). (TAREFA E ESTRUTURA)

1.1) E sobre alguma restrição, você tem conhecimento se existe? (TAREFA)

2) Como você avalia a sua autonomia para instalar aplicativos e sistemas via BYOD para acessar dados corporativos? O que esta autonomia pode proporcionar durante a execução das suas atividades? (PESSOAS)

3) Comente sobre as precauções relacionadas à segurança que você toma com seu(s) dispositivo(s) para fazer o acesso à sistemas e dados da instituição. (TECNOLOGIA)

3.1) Você percebe se existe sistemas de segurança gerenciados pelo Departamento de TI que limitam o seu acesso aos dados e aplicativos corporativos? (TECNOLOGIA)

4) Na sua opinião, qual é a diferença entre usar seu dispositivo pessoal (BYOD) para realizar as atividades de trabalho e usar os dispositivos impostos pela instituição? (TAREFA E PESSOAS)

4.1 Como você avalia o seu desempenho e produtividade na realização das tarefas utilizando seu(s) próprio(s) dispositivo(s)? (PESSOAS E TAREFAS)

5) Você acredita que algum fator pode comprometer o seu desempenho e produtividade ao usar seu dispositivo BYOD para realizar atividades de trabalho? Por exemplo, conversas pessoais com família e amigos em redes sociais ou outros aplicativos podem comprometer suas atividades. (PESSOAS E TAREFAS)

5.1) Tem mais outro fator que você acredita que pode comprometer suas atividades? (PESSOAS E TAREFAS)

6) Você costuma acessar os sistemas da organização via BYOD fora do horário e local de trabalho? Comente sobre isso. (PESSOAS E TAREFAS)

7) Como você avalia a preocupação da alta gerência com a segurança dos dados organizacionais acessados via BYOD? (TAREFA)

8) Comente sobre sua satisfação no trabalho com o uso de dispositivos BYOD? PESSOAS

9) Quando está usando seus próprios dispositivos para realizar atividades de trabalho, com que frequência solicita o suporte do departamento de TI? Comente. (ESTRUTURA)