BYOD: PRÁTICAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO PARA SMARTPHONES EM ÓRGÃOS PÚBLICOS FEDERAIS[1]

CARLOS HENRIQUE DIAS DE OLIVEIRA

Resumo: Este estudo objetivou analisar as políticas de segurança da informação no uso de smartphones pessoais por servidores de órgãos da administração pública. Essa prática recebe o nome de *Bring your own device* (BYOD) ou na tradução como “traga seu próprio dispositivo”. Neste período de surgimento acelerado de novas tecnologias e tendências, cabe refletirmos sobre a importância de técnicas e boas práticas de segurança exigidos pelo mundo digital. Nesta pesquisa foram explorados conceitos dessa nova realidade com o uso do BYOD em órgãos públicos, suas vantagens e desafios, conceitos de segurança da informação, concluindo-se com algumas boas práticas de segurança para o uso desse método. Ao final, abre-se a possibilidade para possíveis novos trabalhos, que visem abranger instituições públicas que exigiam um maior grau de segurança e sigilo.

Palavras-chave: *Smartphones. Segurança. Gestão. BYOD.*

1 INTRODUÇÃO

O dispositivo smartphone é um item presente no cotidiano das pessoas. Se antes eram artigos de luxo, hoje a realidade é outra. A necessidade de se manter conectado e estar sempre junto do celular, apresenta uma nova realidade nos locais de trabalho: funcionários sempre portando seus smartphones e as empresas com dificuldade de proibir o uso durante o trabalho (BORGES e JOIA, 2013).Nesse contexto nasce o *Bring your own device* (BYOD), caracterizado pela permissão da utilização dos dispositivos pessoais durante o serviço e em alguns casos, sendo até incentivado pelo empregador o uso do celular pessoal do empregado na rotina diária, isso ocorre devido a vantagens que esse modelo oferece. (BARBIER, BRADLEY, *et al.*, 2012)

[1] Artigo apresentado como Trabalho de Conclusão do Curso de Especialização em Gestão de Segurança da Informação, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Gestão de Segurança da Informação.

O funcionário deseja acessar os recursos digitais do trabalho em gadgets que ele próprio escolheu, principalmente devido a familiaridade com o mesmo, essa realidade está presente na administração pública, devido principalmente as funcionalidades e tecnologias embarcadas nesses dispositivos (TONI, 2016). E para utilizar o BYOD, necessita-se de um conjunto de diretrizes e normas gerais regulando esse método (DIÓGENES, 2017). A partir disso nasce o problema: quais as melhores práticas na implementação do BYOD, por funcionários de órgãos públicos federais que queiram utilizar smartphones pessoais na sua rotina de trabalho com segurança.

Este estudo tem como objetivo encontrar as melhores práticas de Gestão de Segurança da Informação na utilização do BYOD para smartphones pessoais em órgãos públicos. Um dos passos a ser realizado para alcançar o objetivo geral da pesquisa é conceituar o BYOD. Como segundo objetivo há a necessidade de identificar as vantagens e desafios do BYOD. O terceiro objetivo específico da pesquisa é descrever algumas boas práticas de segurança para o uso desse modelo e um exemplo de uso na administração pública.

As organizações precisam se posicionar quanto a forma de como esse acesso funcionará e quais regras devem ser seguidas para não ocorrer um vazamento de informação reservada (BARBIER, BRADLEY, *et al.*, 2012). Nesse contexto, do ponto de vista teórico, este trabalho contribuiu para apresentar conceitos, definições e ferramentas necessárias aos órgãos que desejam implementar esse método, visto que não foi encontrado nenhum estudo no âmbito nacional que correlacione esse assunto no uso na administração pública.

Para desenvolver este trabalho foi realizada uma pesquisa bibliográfica, com busca do conhecimento em bases textuais, livros, artigos científicos e revistas que apresentem normas bem difundidas sobre a área de Segurança da Informação e que abordam o BYOD, ligando este assunto com as abordagens feitas por diversos autores, como: Baars (2018), Barbier (2012), Diógenes (2017).

2 BYOD (*Bring Your Own Device*), COM SEUS BENEFÍCIOS E DESAFIOS

Buscou-se conceituar BYOD "*Bring Your Own Device*" como uma tendência relativamente nova, que basicamente significa a permissão que a corporação concede aos funcionários para que eles utilizem seus dispositivos pessoais para o trabalho, podendo acessar o banco de dados e infraestrutura da empresa no seu dispositivo pessoal. É uma mudança de mentalidade que está sendo implementada e exige novos comportamentos e adaptabilidade dos gestores de TI. Verifica-se que esse caminho traz novas possibilidades: economia em investimentos em TI, melhor satisfação dos funcionários, diminuição dos custos com treinamento, aumento no processo de inovação da companhia. Certamente se trata de um fator com vantagens, porém há também desafios a serem superados (DIÓGENES e MAUSER, 2016).

Na opinião de Hayes e Kotwica (2013) pode-se dizer que BYOD é a prática de trazer os dispositivos mobiles pessoais como por exemplo: smartphones, laptops, tablets, para dentro da empresa e acessar os dados corporativos, que estão no e-mail e servidores e realizar suas funções diárias. Neste contexto, fica claro que essa modalidade permite uma redução nos investimentos em hardware. O mais preocupante, contudo, é constatar que ainda há casos onde se encontram empecilhos para poder adotar essa rotina. Não é exagero afirmar que o desconhecimento e o medo de se adaptar a novas mudanças é o que mais dificulta a implementação do BYOD. Em todo esse processo pode-se dizer de forma resumida que BYOD é um fenômeno que traz vantagens para a administração, como também para os empregados, mas ainda gera receios na sua implementação.

Conforme explicado é interessante notar que essa tendência pode ocasionar grande economia de meios e investimentos de TI. O relatório anual da Cisco (2016), apontou que pode haver uma economia média de US $ 350 por ano por funcionário com uma política BYOD em vigor. Mesmo assim, parece haver razão para que ainda haja um certo grau de medo ao se adotar o BYOD como uma solução compensadora. Porém 69% dos tomadores de decisões de TI eram a favor do BYOD de acordo com o relatório. É sinal que há uma mudança

na aceitabilidade dessa nova linha, apesar de ainda apresentar uma certa resistência na sua efetivação, dificuldade pode ser vista também em órgãos públicos.

Consoante com o que foi verificado, um estudo da Fortinet (2012), que trabalha na área de segurança de rede, verificou que jovens na idade entre 20 e 29 anos, em um público de 3800 jovens, revelou que 74% dos entrevistados já utilizam diariamente o BYOD em seus locais de trabalho. Trata-se, inegavelmente de um rumo que só tende a crescer. Seria um erro, fechar os olhos para essa nova realidade. Assim, reveste-se de particular importância a adoção de mecanismos e políticas de segurança para mitigar possíveis problemas e proteger as informações e ativos que estão nesses dispositivos móveis, de acordo com Baars, Hintzbergen, *et al.* (2018). Sob essa ótima, os autores deixam claro e ganha particular relevância a observação sobre as medidas de proteção que devem ser implementadas.

Conforme explicado, o BYOD é uma técnica inovadora que busca trazer benefícios tanto para o usuário, como também para o empregador. É importante considerar que melhora o ambiente de trabalho ao permitir que os usuários escolham sua plataforma, além de permitir redução de custos operacionais. A vantagem desta abordagem é dar liberdade ao usuário para que ele possa escolher o aparelho que mais lhe agrade e mude quando achar que tenha necessidade e para a organização a de trazer economia de investimentos na área de TI. Porém exigirá métodos de segurança bem definidos e que se adaptem a realidade da corporação.

Com base na pesquisa da empresa CISCO, de Barbier, Bradley, *et al.* (2012), apontam vantagens similares a outros autores, sendo as seguintes: primeiro, diminui os custos de investimento em TI, principalmente em pequenas empresas; segundo, conforme já mencionado, viabiliza ao funcionário o poder de escolher com qual tecnologia irá querer trabalhar, gerando com isso, uma maior satisfação e aumento da motivação do público em geral; terceiro, abre brecha para aparecimento de tecnologias atuais, que o empregado buscou para

auxilia-lo no seu cotidiano, constituindo, um benéfico para corporação e aumentando a produtividade do funcionário.

Neste contexto, fica claro que BYOD pode trazer vantagens completivas. Porém, nessa mesma pesquisa, constatam-se alguns desafios para a sua implementação. Buscou-se enumera-los: primeiro, com o desafio de segurança de dados, principalmente para o setor de TI, pois a informação pode ficar armazenada em dispositivos móveis, que estão vulneráveis a perdas e roubos; segundo, é uma grande variedade de dispositivos, podendo gerar problemas de compatibilidade; outro exemplo, é a necessidade de ter um rigoroso controle de quais os dispositivos pessoais estão habilitados a acessar a informação, tendo uma lista de dispositivos rotineiramente monitorada e atualizada. Há também a necessidade de uma equipe de TI, altamente treinada, que se atualiza constantemente em cursos e possua dispositivos de hardware/software para se executar a segurança

A melhor maneira de compreender esse processo, é considerar que o BYOD traz benefícios, porém, exige que se superem alguns desafios. Não se trata de desafios insuperáveis, mas de se adaptar a essa nova realidade. Seja porque diminui custos, aumenta a produtividade e a satisfação dos empregados, seja porque impõe a adoção de maior rigor nas regras de segurança da informação. Julgo pertinente trazer à tona principalmente a dificuldade que as empresas nos dias atuais possuem de tentar controlar o uso de parelhos pessoais no horário do expediente.

> Apesar dos executivos não declararem de forma explícita que se sentem escravizados pelo uso da tecnologia, todos, sem exceção, afirmaram que precisam deixar o aparelho ligado para serem encontrados, tanto por colegas de trabalho, como no âmbito particular. Essa obrigação de manter o aparelho ligado foi identificada na fala de J. (masculino, 51 anos): “Até para tomar banho eu levo meu aparelho junto comigo. Virou uma espécie de amigo inseparável. (BORGES e JOIA, 2013, p. 596).

Sendo assim, nota-se a dificuldade de se desvincular do seu dispositivo pessoal. A sociedade está cada vez mais conectada. Busca-se perceber conforme citado no trecho acima, que a inclusão desses aparelhos pode trazer benéficos para ambos os lados. Assim reveste-se de particular importância uma

análise crítica e planejada para a implementação do BYOD de acordo com a realidade e necessidade de cada corporação.

3 A SEGURANÇA DA INFORMAÇÃO E BOAS PRÁTICAS

A origem da segurança da informação surgi com o nascimento da internet. A necessidade de se ligar a rede de computadores, trouxe com ela, atacantes e agentes externos e com isso, a necessidade de protege-la. O DTI (*Departament of Trade and Industry*), localizada no Reino Unido, foi o primeiro órgão internacional a preparar uma norma de Segurança da Informação na década de 80, a ISO 17799 (MANOEL, 2014). Diante do exposto, verifica-se que desde o surgimento das redes de computadores já havia a necessidade de proteger a informação de pessoas externas. Tratando a informação como um ativo, sua perda, reflete em graves prejuízos, esse capítulo se reverte de especial importância na realidade atual.

De acordo com os livros de Thomas Peltier (2015) o primeiro item que devemos atentar no aspecto da segurança é: ter uma política de segurança da informação bem definida que reflita a realidade e as reais necessidades do órgão.

> O primeiro e mais importante aspecto da segurança da informação é a política de segurança. Se a segurança da informação fosse uma pessoa a política de segurança seria o sistema nervoso. Política é a base da segurança da informação da informação, providencia a estrutura e define os objetivos dos demais aspectos da segurança da informação (PELTIER, 2005, p. 17).

Para adotar boas práticas dentro do ambiente tecnológico de um setor público deve ser definida a política de segurança da informação, ela que irá definir o escopo dos controles que serão implementados. Peltier (2005) deixa claro que deve ser um trabalho conjunto entre a equipe de TI e os responsáveis pela administração. Deve ter ampla divulgação e ser de conhecimento de todos os trabalhadores.

Outro quesito necessário, também é ter um plano de tratamento e resposta aos incidentes, para caso haja alguma falha em algum controle de segurança. Para Lima (2018) além desse plano, deve ser realizado um registro

desses incidentes, que possibilitarão uma análise futura, gerando relatórios e identificando falhas, com o levantamento dos possíveis impacto financeiros e custos envolvidos. Com a análise desses dados, poderão ser levantadas medidas para melhorar e aprimorar o controle. Deve possuir também, recursos para monitorar os dispositivos conectados, identificar possíveis ameaças e exclui-las se necessário.

Uma ação que a administração pública deve tomar para reduzir o risco com o uso do BYOD além das políticas de segurança é a implementação de Mobile Device Management ou MDM. Para Fernandes e Abreu (2014), MDM é um software que possibilita gerenciar todos os dispositivos móveis, independentemente de seus sistemas operacionais. Eles listam suas principais funcionalidades: gerenciar os e-mails, o uso de compartilhamento de documentos, as despesas pelo uso dos serviços de aplicativos, configurar a segurança de aplicativos, do browser e dos dispositivos, gerenciar o acesso a sites não permitidos, emitir alertas de violação e administrar as políticas de segurança. Este sistema irá possibilitar a realização do gerenciamento desses dispositivos e com isso melhorar o controle e a segurança da informação.

É interessante também, uma política de uso do ambiente mobile muito bem definida. Nela que serão determinadas todas as regras para o uso de smartphones e outros dispositivos mobile e as implicações em caso de violação. Em concordância com a ISO/IEC27002, da ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (2013), consideram-se necessários alguns requisitos: registro e controle dos dispositivos, a informação deve ser criptografada, restrição ao acesso da informação para usuários não autorizados, realização de bloqueio e exclusão de forma remota. Nesta política deve conter um termo de aceite de uso do ambiente mobile que o usuário deve assinar, que possuirá as regras das políticas do órgão, onde o interessado em utilizar seu equipamento deve concordar com as regras da instituição.

Com relação ao acesso lógico dos dispositivos smartphones, o importante é possuir um método de autenticação, que visa garantir que somente o usuário autorizado acesse a informação e se conecte à rede. De acordo com ISO/IEC

27033-1 (2015) , todo o usuário autorizado deve possuir um ID de acesso restrito única, isto permitirá uma efetividade na ação de controle desses usuários. Caso se vislumbre a permissão para que estes dispositivos se conectem fora da rede interna do órgão, aconselha-se o uso de uma VPN (*Virtual Private Network*), gerando um canal seguro com criptografia.

4 CASO DO EMPREGO DO BYOD NA ADMINISTRAÇÃO PÚBLICA

Um exemplo da utilização de dispositivos pessoais na Administração Pública é o uso do aplicativo EBChat. É uma ferramenta do Exército Brasileiro, para envio e recebimento de mensagens corporativas, com funcionalidades parecidas aos aplicativos Whatsapp ou Telegram. Pode ser baixada tanto pela *Google Play*, como na AppStore, porém a utilização dos recursos não é aberta ao público geral, somente para militares cadastrados podem acessar o sistema.

Como bem nos assegura Pina (2018), que é coronel das Forças Armadas, pode-se dizer que ainda é muito comum a circulação de documentos e informações institucionais fora da rede interna da corporação. Isso decorre principalmente devido ao grande emprego de Smartphones por todos os militares, que em muitos casos, buscam agilizar uma ordem, repassar informações para elementos subordinados de uma maneira mais fácil, coordenar atividades a distância, entre outras. Essa busca de maior velocidade no fluxo das informações causa em alguns casos uma negligência com as regras de segurança, mesmo sendo profissionais que lidam com a segurança.

O mais importante, é constatar que para Pina (2018) "Isso deixa clara a pouca mentalidade de segurança da informação existente, mesmo no universo daqueles que deveriam, no mínimo, dar o exemplo.". É interessante, aliás, afirmar que a forma de se resolver esse problema na segurança é adotar e praticar boas práticas, incorporando individualmente esses hábitos seguros. O Exército Brasileiro, por sua vez, notou essa dificuldade de se controlar esse fluxo de informação corporativas em dispositivos smartphones pessoais, por isso ele criou essa ferramenta para tentar aumentar o grau de segurança dos dados que circulam nesses dispositivos, liberando com isso o emprego do modelo BYOD.

Nesse aplicativo, o militar se submete a certas regras, como cadastramento prévio além de toda a documentação de Políticas de Segurança da Informação estabelecidas. As vantagens dessa ferramenta fornece o uso de criptografia na troca de mensagens, o servidor que hospeda e administra esse fluxo de informação faz parte da infraestrutura do Exército Brasileiro, as mensagens são autodestrutivas com o decorrer do tempo ela se apaga, evitando-se com isso um acúmulo de informação com o passar do tempo em um único aparelho, possui senha para se efetuar o login ao sistema, entre outras funcionalidades que aumentam a segurança no trato das informações da administração pública.

O Cel Rodolfo Tristão Pina ainda reforça a importância dessas iniciativas, mesmo com as dificuldades de se adaptar a essa nova realidade.

> É lógico que essas e outras soluções corporativas, por si sós, não são perfeitas, mas é preciso que se credite confiança nos benefícios de seu uso para a segurança das informações. Dessa forma, torna-se possível a mitigação dos riscos envolvidos na difusão de conteúdo, tanto institucionais, quanto pessoais. O fato de não haver sistemas que ofereçam uma taxa de segurança de 100% não tira o mérito dessas iniciativas, que promovem a melhoria da mentalidade de segurança e criam ambiente propício ao desenvolvimento de outras medidas de proteção mais complexas. Nesse mister, o Exército Brasileiro oferece uma grande contribuição para a segurança institucional e de seus integrantes, com a implantação e difusão do EBMail e do EBChat. (PINA, 2018, p. 1).

O Exército Brasileiro mostra que é possível a utilização de aparelhos próprios mesmo por agentes de segurança, que tratam até com conteúdo sensível e/ou sigiloso de uma forma mais segura. As forças armadas possuem outras iniciativas como o EBMail ou o Sistema Pacificador, que permitem o BYOD para acessar os dados da administração pública. Verificamos com isso, que essa tendência é empregada até em órgãos que demandam maior rigor na segurança.

5 MELHORES PRÁTICAS NA IMPLEMENTAÇÃO DO BYOD, POR FUNCIONÁRIOS DE ÓRGÃOS PÚBLICOS FEDERAIS

Este estudo teve como propósito abordar os resultados da pesquisa sobre as melhores práticas no uso de BYOD em órgãos da administração pública. Verificando abordagens das vantagens e desafios na sua implementação e também verificando desafios para que essa tecnologia seja implementada. A suposição feita a partir do problema quais as melhores práticas na implementação do BYOD, por funcionários de órgãos públicos federais que queiram utilizar smartphones pessoais na sua rotina de trabalho com segurança. Isso porque, para Diógenes e Mauser (2016) o BYOD traz vantagens em sua implementação para ambos os lados, tanto para o empregado com aumento na produtividade, como para a empresa ou órgão, como por exemplo a economia de meios em TI. Mas o autor deixa claro que essa tecnologia carrega consigo precauções de segurança. Por isso, se verifica a necessidade de adoção de políticas de segurança e boas práticas.

Pode-se dizer que o conceito do livro de Diógenes e Mauser (2016) comparado ao conceito do livro de Hayes e Kotwica (2013), são similares e ambos relatam a necessidade de focar nas medidas de segurança. Neste contexto, fica claro que conforme mencionado pelos autores Diógenes e Mauser (2016), para o usuário poder utilizar seu dispositivo, devem ser exigidos dele medidas de proteção e que submeta-se a regras de segurança. Assim, é importante que as corporações que pretendem utilizar o BYOD como recurso, tenham regras bem definidas quanto a utilização e o emprego de dispositivos pessoais.

Pode-se observar após a conceituação do BYOD, que suas maiores vantagens foram a economia na hora de investir em TI e melhora na motivação e satisfação do funcionário, pois permite escolher o aparelho que mais lhe agrada. Também foram constatados alguns desafios a serem superados: dificuldade de realizar a segurança dos dados nos dispositivos pessoais; problemas de compatibilidade com os equipamentos do órgão e maior rigor e controle dos dispositivos autorizados a acessar os serviços disponibilizados, um bom firewall

implementado. Vale destacar, que o medo e a insegurança na hora de implementar esse método atrapalham na hora da sua utilização. Por esse motivo, conforme explicado, Barbier, Bradley, *et al* (2012) falam que não se trata de desafios insuperáveis, mas sim de se adaptar a essa nova realidade. Nesse sentido, o autor deixa explicito que as inseguranças são maximizadas diante da falta de políticas claras de segurança da informação.

No levantamento das boas práticas, foi verificada a necessidade de os órgãos implementarem uma boa política de controle de acesso dos usuários, sendo esta, utilizada de maneira bem rígida, definindo o que o usuário pode acessar e serviços que ele pode utilizar em função do seu cargo. Ressalta-se a importância dessas regras bem definidas e verificadas tanto para o acesso a rede interna como a Internet. Dessa forma, o acesso ao dado é controlado de uma maneira independente do equipamento que está acessando a informação. Outro método importante é a segmentação das redes, como por exemplo, separar as áreas e departamentos em seu grau de importância. Somando as regras e estas segmentações, juntas permitirão um melhor controle e administração da informação, evitando com isso, possíveis vazamentos. Por esse motivo, Diógenes (2017) aborda que o acesso a rede sem fio corporativa deve ser feito de forma controlada e com a inclusão de sensores na rede, para que esta seja monitorada de forma eficiente.

Outra questão levantada, foi com relação se o órgão possui ou não redes sem fio para visitantes. Caso tenha essa disponibilidade, deve-se redobrar ainda mais a atenção, tendo um meio de autenticação por CPF ou cadastro validado, registrando esses acessos e armazenando para possíveis auditorias. É muito importante esse registro pois em caso de crises, pode se verificar o que ocorreu e como. Esse histórico possibilita ainda as verificações de segurança e melhoria no processo de segurança.

Vale destacar também, a necessidade de ter um firewall funcionando e bem configurado. Isto permitirá proteger os sistemas e fazer ligações com os usuários que desfrutam do serviço, dando uma garantia de que somente os usuários autorizados, poderão usufruir dos serviços permitidos. A companhia

Cisco Systems oferece algumas soluções, como por exemplo, o Cisco ISE, que é um mecanismo de identificação de usuários, possibilitando um aumento da visibilidade, um melhor controle do acesso e contendo possíveis ameaças. A empresa Cisco, com seu software Cisco *Identity Services Engine* (ISE), aborda que seu serviço funciona realizando o controle de fornecimento do acesso e melhoramento na política de usuário.

Para alcançar o objetivo geral foi preciso realizar uma pesquisa bibliográfica, visto que a utilização de BYOD em órgãos públicos possui raros exemplos. Em empresas privadas, apesar de mais tempo de aplicação, ainda faltam estudos mais aprofundados e comprovações científicas sobre as vantagens e desafios dessa inclinação. Apesar de poucos estudos, a utilização de smartfones pessoais em ambientes de trabalho não é uma prática exclusiva somente de empresas privadas. Cada vez mais é comum que os servidores públicos utilizem seus telefones durante o trabalho, conectando esses dispositivos na rede interna do órgão. Nesses casos, se torna importante a adoção de boas práticas de segurança da informação. Como esse método ainda é recente, boas práticas surgirão a cada estudo e experimentação, "Como BYOD é cenário ainda recente, muitas regras e boas práticas de segurança poderão ainda ser estabelecidas no futuro. O importante é saber escolher a solução de gerenciamento (MDM) e determinar uma política [...]". (DIÓGENES e MAUSER, 2016, p. 532).

Diante disso, é possível afirmar que mesmo com poucos casos na administração pública, o BYOD apresenta grandes vantagens em sua implementação, trazendo benefícios para ambos os lados, gerando economia de recursos públicos e gerando uma maior satisfação ao funcionário, que trabalhará melhor e como consequência, oferecerá um melhor atendimento para a sociedade. Os desafios podem ser contornados com boas práticas e políticas de segurança bem definidas e implementadas.

6 CONCLUSÕES

O desenvolvimento do presente estudo possibilitou uma análise das boas práticas no uso de BYOD em ambientes de órgãos públicos e as dificuldades

encontradas ao se trabalhar com essa metodologia. Apesar das diferenças e singularidades de cada órgão, todos necessitam de alto sigilo na segurança das suas informações, pois uma perda de um desses dados reservados, pode acarretar um dano financeiro ou prejuízo a imagem da administração pública. As necessidades e características peculiares de cada instituição, aumentam a dificuldade na utilização e padronização única de um modelo na utilização desse método, visto que, em alguns casos, se possui um alto número de usuários, redes com arquiteturas complexas e um grande volume de tráfego de rede, devendo como preceito básico o emprego de boas práticas de segurança.

De um modo geral, o emprego de meios pessoais em ambientes de trabalho se demonstra uma prática comum tanto em grupos corporativos como na administração pública, apesar de muitos casos não estarem regulamentados, o uso do BYOD ainda ocorre. Na literatura analisada, verificam-se grandes benefícios que o emprego desse método pode trazer para uma melhora no serviço público. Constatando-se como principais: a diminuição de investimentos em TI; melhora na satisfação dos empregados resultando em um aumento da produtividade dos servidores públicos. Os principais desafios levantados foram a dificuldade de realizar a segurança dos dados nos dispositivos pessoais, quando esses saem do local de trabalho, problemas de compatibilidade com os equipamentos do órgão e obrigação de um maior rigor e controle dos dispositivos autorizados a acessar os serviços disponibilizados. Há também a necessidade das equipes de TI de se adaptarem a essa nova realidade de acordo com o grau de sigilo e segurança específicos de sua realidade. Em alguns casos peculiares de certos órgãos, pode não ser viável a utilização desse modelo, pois necessitam de um alto grau de sigilo, de uma equipe de TI, altamente treinada, que se atualiza constantemente em cursos e possua dispositivos de hardware/software para se executar a segurança. Foi verificado o emprego do EBchat pelo Exército Brasileiro para que os militares possam mandar mensagem corporativas em dispositivos pessoais.

Dada à importância do tema, torna se necessário o desenvolvimento de projetos que visem a padronização no emprego desse modelo, que possam

desencadear competências e habilidades para garantir segurança a informação, que atendam de uma maneira geral as diferentes necessidades da administração pública e, assim, efetivem o emprego desse modelo de uma forma segura e padronizada. Além dessa regularização, sugere-se uma avaliação sistemática dos riscos de segurança da informação quando da adoção do BYOD na realidade de cada órgão que vislumbre a necessidade de implementar esse modelo. Podendo, com o resultado do levantamento dessas ameaças, verificar quais os impactos nos ativos, quais estão mais expostos e como realizar a segurança do mesmo.

Nesse sentido, a utilização de BYOD em órgãos públicos, requer a definição das melhores práticas e a adesão de Políticas de Segurança bem definidas, que se adaptem a realidade de cada organização. A adoção de boas práticas se mostra como o mínimo necessário para poder utilizar esse modelo de alguma forma segura, trazendo benefícios tanto para a administração pública, como para servidores, resultando em um melhor atendimento para a população.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002 - Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação**. Rio de Janeiro: [s.n.], 2013.

BAARS , H. et al. **Fundamentos de Segurança da Informação:** com base na ISO 27001 e na ISO 27002. 1°. ed. Rio de Janeiro: Brasport, 2018.

BARBIER, J. et al. **BYOD e a virtualização - 10 principais descobertas do estudo do Cisco IBSG**. Cisco IBSG. San Jose, p. 5. 2012.

BORGES, A. P.; JOIA, L. A. Executivos e smartphones: uma relação ambígua e paradoxal. **Revista O&S**, v. 20, p. 505-602, dezembro 2013. Disponivel em: <https://portalseer.ufba.br/index.php/revistaoes/article/view/9127/6572>. Acesso em: 01 abril 2019.

CISCO. Relatório Anual de Segurança da Cisco de 2016, 2016. Disponivel em: <https://www.cisco.com/c/dam/r/pt/br/internet-of-everything-ioe/assets/pdfs/cisco_2016_asr_pt-br.pdf>. Acesso em: 12 Abril 2019.

DIÓGENES, Y. **Certificação de analista em segurança cibernética (CySA+):** Guia preparatório para o exame COMPTIA CS0-001. Rio de Janeiro: Novaterra, 2017.

DIÓGENES, Y.; MAUSER, D. **Certificação Security+:** Da prática para o exame SYO-401. 3°. ed. Rio de Janeiro: Novaterra, 2016.

FARO, C. D. **Administração bancária:** uma visão aplicada. 1°. ed. Rio de Janeiro: FGV, 2015.

FERNANDES, A. A.; ABREU, V. F. D. **Implantando a Governança de TI - 4ª Ed.:** Da estratégia à Gestão de Processos e Serviços. 4°. ed. Rio de Janeiro: Brasport, 2014.

FORTINET(R) Global Survey Reveals 'First Generation' BYOD Workers Pose Serious Security Challenges to Corporate IT Systems. **Fortinet**, 2012. Disponivel em: <https://investor.fortinet.com/news-releases/news-release-details/fortinetr-global-survey-reveals-first-generation-byod-workers>. Acesso em: 08 Abril 2019.

HAYES, ; KOTWICA,. **Nine Practices of the Successful Security Leader:** Research Report. 1°. ed. Waltham: Elsevier, 2013.

ISO - INTERNATIONAL ORGANIZATION FOR STANDARDIZATI. **ISO/IEC 27033-1 - Information technology -- Security techniques -- Network security-- Part 1:** Overview and concepts. [S.l.]: [s.n.], 2015.

LIMA,. **Gestão da segurança e infraestrutura de tecnologia da informação**. 1°. ed. São Paulo: Senac, 2018.

MANOEL, S. D. S. **Governança de Segurança da Informação:** Como criar oportunidades para o seu negócio. 1°. ed. Rio de Janeiro: Brasport, 2014.

MEIRELLES, F. S. **FGV EAESP**, 2018. Disponivel em: <https://eaesp.fgv.br/sites/eaesp.fgv.br/files/pesti2018gvciappt.pdf>. Acesso em: 10 abril 2019.

P. DE LAS CUEVAS, A. M. et al. Corporate security solutions for BYOD: A novel user-centric and self-adaptive system. **Computer Communications**, 68, 1 September 2015. 83-95.

PELTIER, T. R. **Information Security Risk Analysis**. 2°. ed. Cleveland: CRC Press, 2005.

PINA, R. T. http://eblog.eb.mil.br. **EBlog - BLOG do Exército Brasileiro**, 2018. Disponivel em: <http://eblog.eb.mil.br/index.php/menu-easyblog/ebmail-e-ebchat-exemplos-de-seguranca-no-trato-das-informacoes-pessoais-e-institucionais-nos-meios-eletronicos.html>. Acesso em: 29 abril 2019.

RASCÃO, J. P. **Da Gestão Estratégica à Gestão Estratégica da Informação:** Como aumentar o tempo disponível para a tomada de decisão estratégica. Rio de Janeiro: E-papers, 2006.

SÊMOLA, M. **Gestão da Segurança da Informação - Uma Visão Executiva**. 2ª. ed. Rio de Janeiro: Elsevier, 2014.

SWINHOE, D. Os 8 maiores vazamentos de dados de 2018. **Computer World**, 2018. Disponivel em: <https://computerworld.com.br/2018/10/31/os-8-maiores-vazamentos-de-dados-de-2018/>. Acesso em: 10 abril 2019.