ESTUDO DO USO DE DISPOSITIVOS MÓVEIS PESSOAIS EM AMBIENTE CORPORATIVO NO ÂMBITO DA SEGURANÇA DA INFORMAÇÃO[1]

Pedro Moritz de Carvalho Neto[2]

Resumo: Alguns fatores relacionados ao modo de vida da sociedade moderna motivaram a produção deste artigo. Um destes fatores é o uso intenso e cada vez mais difundido dos dispositivos móveis pessoais. Outro fator é o valor da informação, cada vez maior, em todas as áreas e segmentos das atividades humanas. Os dispositivos móveis atuais possuem grande capacidade de armazenamento, considerável poder de processamento e diversas possibilidades de conectividade. No entanto, o uso inadequado destas poderosas ferramentas pode afetar gravemente a segurança da informação em ambiente corporativo. O objetivo deste artigo é identificar o perfil de uso pessoal dos dispositivos móveis no ambiente corporativo e procurar saber qual é o grau de importância que as empresas dão à esta questão. Este trabalho foi baseado em uma pesquisa empírica e pura, do tipo exploratória. A técnica utilizada para a coleta dos dados primários foi a aplicação de um questionário aos colaboradores das empresas participantes da amostra. Os principais resultados encontrados na pesquisa são o uso intenso deste tipo de equipamento no ambiente corporativo e a insuficiente aplicação de políticas formais que pudessem prevenir ou mitigar eventuais problemas na segurança da informação.

Palavras-chave: Tecnologia da Informação. Segurança da Informação. Dispositivos Móveis.

1 INTRODUÇÃO

Diversos fatores contribuem para que os dispositivos móveis (*e.g. tablets*, *notebooks*, *smartphones*, etc) sejam cada vez mais utilizados. Entre estes fatores podemos citar, principalmente, a redução de custo destes equipamentos pelo ganho de escala e pelas novas tecnologias, o que os tornou populares e acessíveis a todas as classes sociais. Além disso, a necessidade de mobilidade e conectividade, criadas pelo modo de vida do homem moderno, são satisfeitas por estes equipamentos. Relacionamentos humanos, de vários tipos, são afetados pelo uso destes dispositivos.

---

1 Artigo apresentado como Trabalho de Conclusão do Curso de Especialização em Gerência de Projetos de Tecnologia da Informação, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Gerência de Projetos de Tecnologia da Informação.

2 Tecnólogo em Gestão da Tecnologia da Informação (UNISUL, 2010) e discente do Curso de Especialização em Gerência de Projetos de Tecnologia da Informação (UNISUL).

Negócios são realizados através de dispositivos móveis, assim como a produção da informação e seu consumo são influenciados diretamente pelo seu uso.

Como não podia ser diferente, o uso adequado de dispositivos móveis também produz impacto positivo na maneira como o trabalho é realizado, tornando-o mais eficiente e produtivo. São inúmeras as vantagens que podem ser obtidas por meio do uso de dispositivos móveis. Podemos citar, dentre outras tantas, a facilidade de acesso à informação, o aumento da produtividade e a redução de custos operacionais.

No entanto, apesar das grandes vantagens apresentadas pelo uso de dispositivos móveis, há um lado negativo. Como qualquer tecnologia disponível, seu uso pode trazer, além dos benefícios, problemas que precisam ser contemplados.

Dispositivos móveis podem trazer ameaças para dentro do ambiente corporativo devido à criação de vulnerabilidades nos sistemas que processam, transportam ou armazenam a informação. Além disso, dispositivos móveis podem ser perdidos ou furtados mais facilmente, o que poderia fazer com que dados presentes nestes dispositivos pudessem ser acessados indevidamente. Grande capacidade de armazenamento e diversas tecnologias de conectividade tornam estes equipamentos bastante práticos e adequados à tarefa de transportar dados.

Cabe lembrar que os dados internos das corporações são cada vez mais sensíveis, sendo que o acesso indevido a estes dados pode gerar perdas financeiras (*e.g.* projetos, carteira de clientes) e até mesmo perdas indiretas, devido à eventuais problemas legais (*e.g.* violação de confidencialidade de dados de clientes, fornecedores e colaboradores). Uma única perda de dados que seja conhecida pelo público, sem a comunicação correta e o devido gerenciamento de crise, pode por a perder a confiança do mercado, clientes, investidores e funcionários, causando enormes perdas financeiras e de imagem à corporação. Desta maneira, ficam as questões: existem ações por parte das empresas que demonstrem sua preocupação sobre o uso deste tipo de equipamento em ambiente corporativo? O uso deste tipo de equipamento realmente é tão intenso assim, a ponto de justificar esta preocupação?

Os dados analisados neste trabalho resultam da aplicação de um questionário, apresentado a 124 pessoas de 77 diferentes empresas. Estas empresas pertencem a diversos segmentos de atuação, como comércio, indústria e prestação de serviços, tanto do setor público quanto do setor privado, e se localizam na Região Metropolitana de Florianópolis. Para a criação deste questionário e para a coleta de respostas foi utilizada a ferramenta online Survio (http://www.survio.com/). O questionário submetido pode ser acessado no endereço https://www.survio.com/survey/d/A1J8L4R9L4Y1P9S4X. No período de coleta de dados, entre 23/03/2017 e 30/03/2017, 56 respondentes completaram a pesquisa, gerando os dados analisados no presente trabalho.

2 DISPOSITIVOS MÓVEIS PESSOAIS E A SEGURANÇA DA INFORMAÇÃO

Considerar a informação como um ativo valioso, que precisa ser preservado, não é um fenômeno moderno. Desde o início da história de nossa civilização, o domínio da informação sempre representou um diferencial estratégico. Um exemplo disso (COUTO, 2008, p. 15-17) é a Cifra de César, técnica de criptografia utilizada pelo cônsul e ditador romano Caio Júlio César (100 a.C. - 44 a.C.) para se comunicar de maneira segura com seus generais. Este é apenas um exemplo de como a informação, há mais de dois mil anos, já possuía valor e demandava processos e técnicas para sua proteção.

A partir do início do período chamado **Sociedade pós-industrial** ou **Era da informação**, termos cunhados respectivamente pelos professores Daniel Bell e Peter Drucker, fica evidente que a informação passa a ser um bem importantíssimo e de grande valor para toda a sociedade. Diante do grande valor que a informação possui, é necessário que exista um conjunto de mecanismos e processos que proporcionem segurança adequada a este ativo. A este conjunto organizado de mecanismos e processos denominamos Segurança da Informação. Conforme Coelho *et al.* (2014, p. 2):

> Segurança da informação compreende a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros (intencionais ou não) e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança.

A segurança da informação é caracterizada por LENTO (2014) pela preservação das seguintes propriedades:

a) **Confidencialidade**: a segurança de um sistema computacional não deve admitir que informações sejam descobertas por qualquer pessoa não autorizada. A confidencialidade garante a privacidade das informações sensíveis em ambientes computacionais.

b) **Integridade**: a segurança de informação deve sempre manter a integridade da informação armazenada. Logo, manter a integridade dos dados de um sistema significa que esses não terão as suas informações corrompidas, seja de forma acidental ou intencional, via pessoas não autorizadas.

c) **Disponibilidade**: Consiste na capacidade de manter disponível para os usuários do sistema os dispositivos de software e hardware. A disponibilidade assegura que um usuário autorizado tenha acesso ininterrupto à informação.

Além destes conceitos, conhecidos por CID (sigla para Confidencialidade, Integridade e Disponibilidade), Peixinho *et al.* (2013, p. 4) cita outros conceitos auxiliares, como:

d) **Autenticidade**: garantia de que uma informação, produto ou documento foi elaborado ou distribuído pelo autor a quem se atribui.

e) **Legalidade**: garantia de que as ações sejam realizadas em conformidade com os preceitos legais vigentes e que seus produtos tenham validade jurídica.

f) **Não repúdio**: conceito muito utilizado quando tratamos de certificação digital, onde o emissor de uma mensagem não pode negar que a enviou. As tecnologias de certificação digital e assinatura digital são exemplos que propiciam essa condição.

g) **Privacidade**: conceito amplo, que expressa a habilidade de um indivíduo em controlar a exposição e a disponibilidade de informações acerca de si. Com o crescimento dos mecanismos de busca, bancos de dados e informações publicadas na internet e redes sociais, esse conceito tem sido muito discutido em fóruns específicos.

Segundo LENTO (2014), algumas definições relacionadas à segurança da informação são importantes para a contextualização a respeito deste tema:

a) **Vulnerabilidade**: é uma condição existente em software ou hardware que pode resultar em perda de confidencialidade, disponibilidade ou integridade das informações. As vulnerabilidades também podem ser criadas por configurações incorretas do computador ou de segurança. As ameaças exploram as vulnerabilidades, o que resulta em possíveis danos para o computador ou dados.

b) **Ameaça**: é tudo aquilo que tem potencial para causar danos aos ativos de informação (ex.: invasão, indisponibilidade de serviços etc.). A ameaça pode ser vista como um risco, esse risco pode ser uma pessoa, algo (um dispositivo defeituoso), ou um evento (incêndio, terremoto etc.) que venha a explorar a vulnerabilidade do sistema.

c) **Ataque**: é a concretização de uma ameaça. Um ataque pode ser definido como a efetivação de uma ameaça sobre uma vulnerabilidade.

Devido à relevância que a segurança da informação assumiu com o passar dos anos, diversos comitês foram criados e normas e documentos foram produzidos, na tentativa de prover critérios e processos consistentes para a gestão da segurança da informação.

Neste contexto surge, em outubro de 2005, a norma ISO/IEC 27001:2005. Publicada pelas instituições ISO (*International Organization for Standardization* ou Organização Internacional de Normalização) e IEC (*International Electrotechnical Commission* ou Comissão Eletrotécnica Internacional), a ISO/IEC 27001 é uma norma internacional que padroniza a implementação de um ISMS (*Information Security Management System* ou sistema de gestão da segurança da informação). A ISO/IEC 27001 descreve como colocar em prática um sistema de gestão de segurança da informação avaliado e certificado de forma independente. Esta norma foi construída usando como base a norma Britânica BS 7799-2 (*British Standard* 7799, parte 2, versão de 2002), publicada pelo BSI (*British Standards Institution* ou Instituição de Normas Britânicas).

A ISO/IEC 27001 faz parte da família ISO/IEC 27000, que inclui outras normas e documentos de referência relacionados à gestão da segurança da informação. Em 2006 a ABNT (Associação Brasileira de Normas Técnicas) elaborou a NBR ISO/IEC 27001:2006, que é uma tradução exata da ISO/IEC 27001:2005. A versão atual da norma ISO/IEC 27001 é a ISO/IEC 27001:2013, que também possui uma tradução exata publicada pela ABNT, a NBR ISO/IEC 27001:2013. Uma das ferramentas mais importantes para a segurança da informação no ambiente corporativo é a política de segurança da informação, definida por Dantas (2011, p. 131):

> Nesse sentido, pode-se definir a política de segurança da informação como: um documento que estabelece princípios, valores, compromissos, requisitos, orientações e responsabilidades para com a segurança da informação. A sua forma, escopo e detalhes estão diretamente relacionados com as atividades de negócios e decisão da organização do nível e padrão de segurança que se pretende alcançar.

As diretrizes para a especificação de uma política de segurança da informação também estão descritas em uma norma, a ISO/IEC 27002:2013, mais especificamente em sua Seção 5. Esta norma também possui tradução exata publicada pela ABNT, a NBR ISO/IEC 27002:2013.

Tratando em específico dos dispositivos móveis (*e.g. smartphones*, *tablets* e *notebooks*), há uma série de questões relacionadas à segurança da informação quando abordamos o uso deste tipo de equipamento em ambiente corporativo. O CERT.br (Centro de Estudos, Resposta e Tratamentos de Incidentes de Segurança no Brasil) listou, em sua Cartilha de Segurança para Internet[3], uma série de questões relacionadas à segurança em dispositivos móveis. Além das boas práticas, como as listadas pelo CERT.br, há uma série de abordagens corporativas que também tem o objetivo de melhorar a segurança da informação relacionada ao uso destes dispositivos.

Uma destas abordagens é o BYOD (sigla para *Bring Your Own Device* ou Traga Seu Próprio Dispositivo). Esta abordagem consiste em, basicamente, permitir e/ou incentivar que os colaboradores de uma organização tragam seus próprios equipamentos pessoais para o ambiente corporativo, podendo utilizar estes equipamentos em suas atividades de acordo com certas diretrizes. Segundo Taurion (2012, p. 1):

---

3 Disponivel em: <https://cartilha.cert.br/dispositivos-moveis/>.

> A consumerização de TI é um fato e com este fenômeno surge o movimento chamado de BYOD, ou Bring Your Own Device. Isto significa que os funcionários estão usando tablets e smartphones no seu dia a dia e querem trazê-los para seus ambientes de trabalho. O BYOD libera os funcionários para usar os dispositivos que mais os agradam para a realização das suas tarefas profissionais. Como os consumidores finais estão hoje à frente da vanguarda tecnológica, as empresas perceberam que é muito mais negócio abraçar essa ideia do que proibir. Afinal, elas não podem fechar os olhos para esta tendência, que segundo analistas de mercado, é impossível de bloquear.

No entanto, cabe observar que estes equipamentos pessoais, como quaisquer outros, podem produzir (de maneira intencional ou não) vulnerabilidades na segurança da informação ou até mesmo colaborar ativamente em ataques no ambiente corporativo. Diversas literaturas sugerem modelos para a adoção do modelo de BYOD, de maneira a aproveitar os benefícios do uso de dispositivos móveis pessoais em ambiente corporativo, mantendo a segurança da informação em níveis aceitáveis. Dentre as diversar literaturas que propõem soluções para este tema, podemos citar o artigo *Guidelines for Designing a BYOD Strategy That Succeeds* (DIOGENES, 2014), que sugere um modelo de BYOD baseado no tratamento adequado de quatro itens, aos quais o autor se refere como "componentes": os dispositivos, os usuários, as aplicações e os dados.

Outras abordagens surgiram para lidar com o problema do uso de dispositivos móveis pessoais no ambiente corporativo. Além do BYOD, podemos citar, entre outras tantas, o COPE (sigla para ***Corporate Owned, Personally Enabled*** ou **Propriedade da Empresa, Pessoalmente Habilitado**). Segundo Mobiltec (2015, p. 1):

> Essa é a estratégia mais conservadora, indicada para empresas que possuem maior necessidade de ter controle total sobre as operações externas e o uso de dispositivos. Nesse cenário, a empresa adquire os dispositivos e fornece aos colaboradores para uso exclusivo do trabalho.

Além do COPE, há uma alternativa intermediária, o CYOD (sigla para ***Choose Your Own Device*** ou **Escolha Seu Próprio Dispositivo**). Também conforme Mobiltec (2015, p. 1):

> O caminho do meio. O CYOD é um meio termo entre a rigidez do COPE e a liberdade total do BYOD. Trata-se de uma estratégia na qual a empresa oferece algumas opções de dispositivos para seus colaboradores, com sistema operacional e características determinadas pela empresa, mas que podem ser utilizados para fins pessoais.

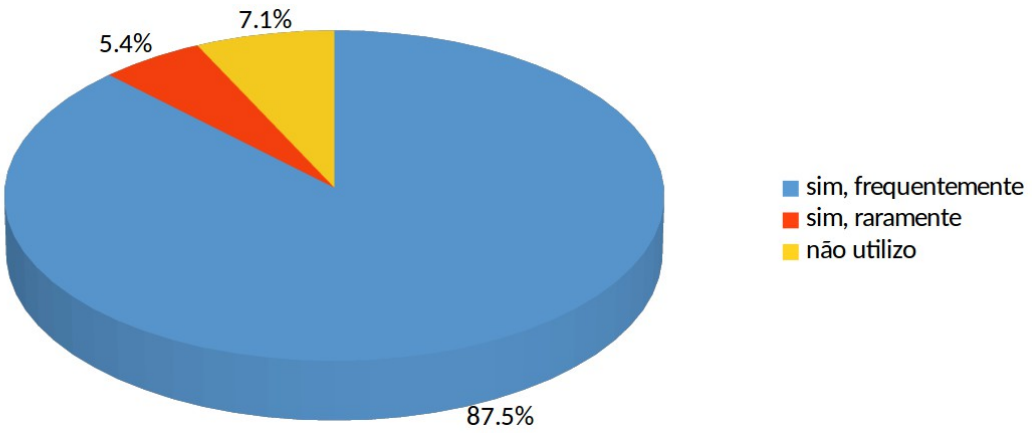
Como se percebe, há uma preocupação do mercado em definir modelos e abordagens que auxiliem no uso seguro de dispositivos móveis em ambiente corporativo. Problemas relacionados à legislação trabalhista, questões patrimoniais, produtividade e engajamento do colaborador também são motivadores para a adoção de modelos eficazes que favoreçam o uso destes tipo de dispositivo em atividades profissionais. No entanto, a questão da segurança da informação aparenta ser a mais relevante de todos os fatores envolvidos.

2.1 ANÁLISE E CONSIDERAÇÕES A RESPEITO DOS DADOS RECEBIDOS

A presente ferramenta de coleta de dados foi planejada para, de maneira simples, instigar o respondente a apresentar duas informações principais: a) se o respondente fazia uso de dispositivos móveis pessoais dentro no seu ambiente de trabalho e b) se a empresa para a qual o respondente presta serviço possuía alguma política em relação a este assunto. Uma terceira questão foi apresentada ao respondente, procurando saber o nível de restrição da política de segurança da informação, caso houvesse. Por fim, uma quarta questão, de resposta aberta e não obrigatória, foi também apresentada buscando contribuições ou questionamentos do respondente.

De maneira propositada não foi citado no questionário o termo **Segurança** ou a expressão **Segurança da Informação**. A intenção principal era saber se o dispositivo móvel era utilizado naquele contexto, sem associar este uso à uma eventual vulnerabilidade e/ou ameaça na segurança da informação da organização.

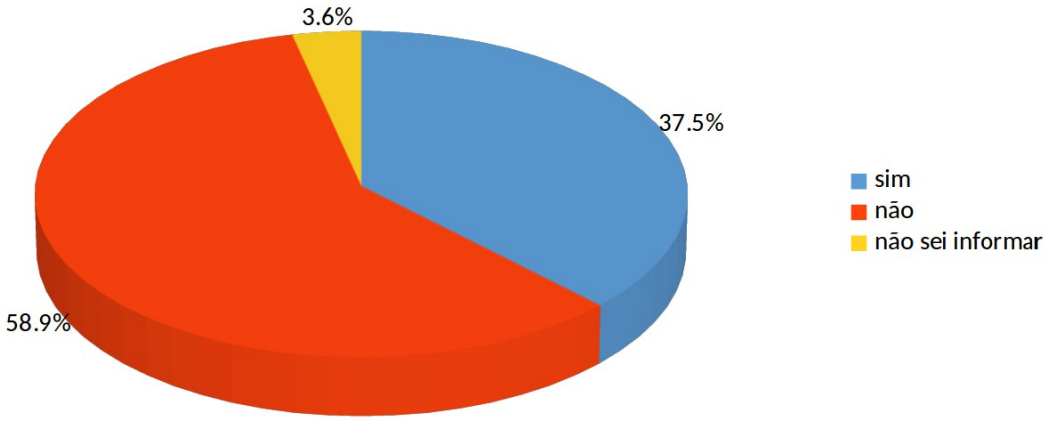
Gráfico 1 - Você utiliza dispositivos móveis pessoais para acessar informações dentro do ambiente da empresa?



Fonte: elaboração do autor, 2017.

Analisando o Gráfico 1 observa-se que a grande maioria dos respondentes (87,5 %) utiliza com frequência este tipo de equipamento nas dependências da empresa. Cabe lembrar que, nos casos em que não há o devido tratamento desta situação, o uso de dispositivos móveis pessoais no ambiente da empresa tanto pode ser um vetor para a entrada de vírus e/ou demais artefatos de código malicioso, quanto pode representar um vetor de saída para fuga de dados e informações sensíveis, representando graves riscos como a perda de receita ou o dano de ativo intangível, como a imagem e a reputação da empresa, por exemplo.

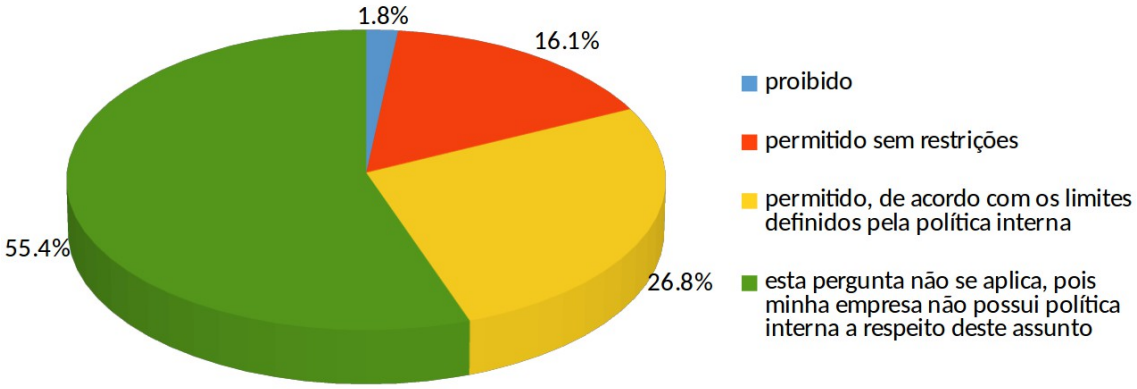
Gráfico 2 - A empresa onde você trabalha possui algum tipo de política interna a respeito do uso de dispositivos móveis pessoais no ambiente corporativo?



Fonte: elaboração do autor, 2017.

Analisando o Gráfico 2 é possível observar que a maioria dos respondentes (58,9 %) não possui uma política interna que explicitamente regule o uso deste tipo de equipamento no ambiente de trabalho. Podemos explicar este número, somado ao número de respondentes (3,6 %) que relataram não saber informar se havia ou não uma política, por diversas hipóteses. Uma delas seria realmente a falta de priorização do assunto por parte das corporações, isto devido à falta de orçamento, falta de patrocinadores internos, ausência de eventos e/ou informação que gerasse preocupação em relação à segurança da informação no aspecto dos dispositivos móveis. Outra hipótese que pode explicar este número pode ser a falta de um *endomarketing* adequado, para os casos em que a empresa possui uma política interna a respeito do assunto (ainda que rudimentar), mas não tenha divulgado adequadamente este fato aos seus colaboradores.

Gráfico 3 - Caso sua empresa possua política interna a respeito deste assunto, o uso de dispositivos móveis pessoais no ambiente da empresa, de acordo com esta política, é:



Fonte: elaboração do autor, 2017.

Uma das análises possíveis em relação ao Gráfico 3 é que, dentre os respondentes que estão sob a diretriz de uma política interna a respeito do assunto, a maioria (26,8 %) está sujeita a algum tipo de controle (**permitido, de acordo com os limites definidos pela política interna**). Por outro lado, uma parte da população pesquisada (16,1 %) afirma que a política interna a que está sujeito permite o uso deste tipo de equipamento de maneira irrestrita, o que sugere falta de preocupação da organização com os perigos potenciais desta prática. Outro dado que desperta preocupação é que a maioria dos respondentes (55,4 %) relata que **esta pergunta não se aplica, pois minha empresa não possui política interna a respeito deste assunto**.

Uma 4ª questão, de tipo aberto, foi apresentada no sentido de coletar informações que pudessem eventualmente enriquecer a discussão, deixando livre a contribuição dos respondentes. Algumas observações recebidas nesta questão são bastante interessantes, sugerindo abordagens para resolver o problema de segurança da informação relacionado ao uso de dispositivos móveis pessoais em ambiente corporativo.

Uma destas abordagens, a BYOD, foi citada em um comentário enviado nesta 4ª questão. Conforme foi conceituado anteriormente, nesta abordagem os colaboradores são incentivados a fazer uso de seus equipamentos pessoais dentro do ambiente da empresa, de acordo com uma política que explicitamente define o que pode e o que não pode ser feito.

A abordagem COPE também foi citada em um comentário nesta 4ª questão. Nesta abordagem, os equipamentos móveis pessoais do colaborador são fornecidos pela empresa, que é responsável por equipá-los com recursos que minimizem as eventuais ameaças na segurança da informação da empresa. Além disso, políticas rígidas podem ajudar no uso adequado destes dispositivos, trazendo os riscos de segurança a níveis aceitáveis e perfeitamente gerenciáveis.

Outros comentários recebidos nesta 4ª questão citam a baixa produtividade dos colaboradores que utilizam dispositivos móveis pessoais, principalmente no que diz respeito ao acesso às redes sociais, em ambiente corporativo. Outro comentário sugere que o ideal seria não impor nenhuma restrição ao uso deste tipo de equipamento no ambiente de trabalho. As impressões coletadas desta 4ª questão são bastante variadas: enquanto algumas soam mais restritivas e preocupadas com a questão da produtividade e da segurança da informação, outras atribuem maior importância à liberdade do funcionário e à sua satisfação no ambiente de trabalho.

De uma maneira geral, é possível observar que é intenso o uso de dispositivos móveis pessoais em ambiente corporativo. Por outro lado, o grande número de respondentes que informaram não trabalhar sob diretrizes explícitas a respeito deste assunto significa que não há uma preocupação (ou ao menos uma priorização) da parte das empresas no sentido de reduzir os riscos associados a este cenário. Uma sugestão seria que as empresa implementassem, se não uma política de segurança da informação nos moldes das normas vigentes, ao menos diretrizes básicas que definissem o que pode e que não pode ser feito pelo colaborador em relação ao assunto desta pesquisa.

3 CONCLUSÕES

O uso intenso de dispositivos móveis pessoais em ambiente corporativo não é apenas uma hipótese. É um fato constatado de maneira informal pela observação do cotidiano, mas também pelos dados coletados e analisados em pesquisas acadêmicas e de mercado, como a realizada neste trabalho. Se este uso acontece em um contexto onde não há política de segurança da informação ou onde esta é incipiente, produz-se um cenário propício à criação de vulnerabilidades. Por outro lado, a simples proibição do uso destes equipamentos em ambiente corporativo pode ser inócua ou até mesmo gerar

problemas de relacionamento entre colaboradores e as hierarquias superiores. Uma alternativa viável seria aproveitar o potencial destes equipamentos e do engajamento do colaborador através da criação de políticas que estimulem o uso consciente dos dispositivos móveis pessoais, sem abrir mão de níveis de segurança. Um achado importante neste trabalho é o fato de que a maioria das empresas pesquisadas não possui este tipo de política implementada, mesmo que de maneira rudimentar. A existência deste tipo de diretriz, definindo abordagens e orientando colaboradores a respeito do uso adequado deste tipo de equipamento, reduziria os riscos relacionados à perda e exposição de dados sensíveis. As causas para este tipo de perda são as mais diversas, podendo ser intencionais ou não-intencionais, seja a trivial mas não menos perigosa introdução de um vírus na rede ou até mesmo um ato planejado de espionagem industrial. É possível concluir que há, neste *gap*, uma oportunidade para a oferta de treinamentos, consultorias e serviços técnicos relacionados ao uso de dispositivos móveis no contexto da segurança da informação. Infelizmente, é comum que as organizações reservem parte de seu *budget* para serviços e produtos ligados à segurança da informação apenas após a ocorrência de perdas, tangíveis e intangíveis, decorrentes de ataques à vulnerabilidades.

Uma sugestão para trabalhos futuros é a criação de um modelo simplificado de política de segurança que contemple o uso de dispositivos móveis pessoais. Este modelo deve estabelecer diretrizes para o uso deste tipo de equipamento em ambiente corporativo, de maneira a garantir níveis adequados na segurança da informação, incluindo a criação de material de conscientização e treinamento de colaboradores. Outra sugestão de trabalhos futuros seria um estudo ou comparação de sistemas e/ou soluções de MDM (sigla para ***Mobile Device Management*** ou **Gerenciamento de Dispositivos Móveis**). Esta sigla se refere aos produtos de mercado que permitem o gerenciamento remoto de dispositivos móveis, permitindo, entre outras ações, a distribuição e atualização de softwares, o rastreamento de componentes de software e hardware, o *backup* e a restauração de dados, o bloqueio de equipamentos perdidos/furtados, além do gerenciamento da segurança deste tipo de equipamento.

REFERÊNCIAS

COELHO, Flávia Estélia Silva; ARAÚJO, Luiz Geraldo Segadas de; BEZERRA, Edson Kowask. **Gestão da Segurança da Informação - NBR 27001 e 27002**. Rio de Janeiro: Escola Superior de Redes, RNP, 2014.

COUTO, Sérgio Pereira. **Códigos & Cifras da Antiguidade à Era Moderna**. Rio de Janeiro: Novaterra, 2008.

DANTAS, Marcus Leal. **Segurança da Informação: Uma Abordagem Focada em Gestão de Riscos**. Olinda: Livro Rápido, 2011.

DIOGENES, Yuri. **Guidelines for Designing a BYOD Strategy That Succeeds**. *ISSA Journal*, p 22-26, mar. 2014.

LENTO, Luiz Otávio Botelho. **Gestão de segurança**. Livro digital. Palhoça: UnisulVirtual, 2014.

MOBILTEC. **COPE, BYOD E CYOD: Como escolher a estratégia de mobilidade mais adequada para sua empresa.** 2015. Disponível em: <http://www.mobiltec.com.br/Noticias/Ler/byod-cyod-cope/>. Acesso em: 2 maio 2017.

PEIXINHO, Ivo de Carvalho; FONSECA, Francisco Marmo da Fonseca; LIMA, Francisco Marcelo Marques. **Segurança de Redes e Sistemas**. Rio de Janeiro: Escola Superior de Redes, RNP, 2013.

TAURION, Cezar. **Como Utilizar o BYOD na Prática**. 2012. Disponível em: <https://imasters.com.br/artigo/25377/tendencias/como-utilizar-o-byod-na-pratica/>. Acesso em: 4 maio 2017.