Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Segurança da Informação

A CONSUMERIZAÇÃO E O USO DE DISPOSITIVOS MÓVEIS PESSOAIS PARA FINS DE TRABALHO (BYOD)

JOSÉ PAULO DE CARVALHO CAMBRAIA

Americana, SP
2013

Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Segurança da Informação

A CONSUMERIZAÇÃO E O USO DE DISPOSITIVOS MÓVEIS PESSOAIS PARA FINS DE TRABALHO (BYOD)

JOSÉ PAULO DE CARVALHO CAMBRAIA
jpcambraia2@gmail.com

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Me. Leandro Halle Najm.

Área: Segurança da Informação

Americana, SP
2013

BANCA EXAMINADORA

Prof. Me. Leandro Halle Najm (Orientador)

Prof. Me. Carlos Henrique Sarro

Prof. Me. Alexandre Garcia Aguado

DEDICATÓRIA

Dedico este trabalho a minha querida Ana Lúcia, que foi aquele anjo enviado pelos céus no momento mais difícil da minha vida.

AGRADECIMENTOS

Agradeço a Deus, a meus pais e à minha avó em primeiro lugar, pelo amor e pelo incondicional apoio em todos os momentos da vida. Agradeço eternamente também àquelas pessoas que, embora seja impossível nominar todas, de alguma forma me auxiliaram a conseguir chegar até aqui.

RESUMO

O presente texto caracteriza a consumerização, também conhecida como BYOD – *Bring Your Own Device* –, que é a utilização no trabalho de tecnologias disponíveis ao consumidor comum, abordando mais especificamente o uso de dispositivos móveis no ambiente corporativo. Primeiramente conceituaremos a consumerização como tecnologia inovadora com implicações sociais, observando a mudança que isto deve acarretar na gestão estratégica do setor de TI das organizações. Então caracterizaremos o programa BYOD, que pode ser considerada como a política de segurança da informação com relação aos dispositivos móveis da empresa, abordando o gerenciamento de aspectos relativos à propriedade, produtividade, suporte e segurança.

Palavras Chave: Consumerização, BYOD, dispositivos móveis.

ABSTRACT

The present text characterizes consumerization, also known as BYOD – Bring Your Own Device –, which is the usage of consumer technologies in work, more specifically the usage of mobile devices in corporative environment. In the first place, we'll conceptualize consumerization as an innovative technology with social implications, observing the changes that might take place in the strategic management of organization's IT's department. Then we'll characterize BYOD, which may be considered as a security policy that concerns about the mobile devices, mentioning aspects related to property, productivity, support and security.

Keywords: *Consumerization, BYOD, mobile.*

LISTA DE FIGURAS:

FIGURA 1 – Consumerização como tecnologia disruptiva.....17

SUMÁRIO:

1. INTRODUÇÃO 10
2. CONSUMERIZAÇÃO 12
2.1. Aspecto social da consumerização 12
2.2. Consumerização como tecnologia disruptiva 15
2.3. Conformidade 18
2.4. Aspecto comercial do BYOD 19
2.5. Papel da TI 22
3. PROGRAMA *BRING YOUR OWN DEVICE* – BYOD 25
3.1. Propriedade 26
3.2. Produtividade 31
3.3. Suporte 37
3.4. Segurança 42
4. BYOD NA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO 46
4.1. Estudo de Caso: Instituto Mackenzie de São Paulo 51
4.2. Estudo de Caso: SENAC de São Paulo 53
5. CONSIDERAÇÕES FINAIS 56
6. REFERÊNCIAS BIBLIOGRÁFICAS 59

1. INTRODUÇÃO

O objetivo geral deste trabalho foi fazer uma caracterização da consumerização, termo aportuguesado da palavra inglesa *consumerization*, também conhecida como BYOD – *Bring Your Own Device*. É um fenômeno que teve seu início há poucos anos, e, como diz Cezar Taurion, diretor de novas tecnologias aplicadas da IBM – *International Business Machine* – "não existem livros de referência de melhores práticas consagradas". É necessário criar estes livros (CIO, 2013b).

Consumerização, para fins deste trabalho, é o uso de dispositivos móveis pessoais para o acesso de informação particular ou corporativa, dentro ou fora do local de trabalho. Com relação ao BYOD, este será tratado como um programa que implementa a política de segurança da informação da empresa com relação a este uso.

Dispositivo móvel será definido como toda unidade computacional que possua dispositivo para conexão em redes de computadores e bateria interna que lhe permita ser carregado como, por exemplo, *smartphones, tablet's, notebooks, netbooks, ultrabooks*, PDA's etc. Além disso, estes dispositivos podem ser híbridos, como o *smartphone*, que agrega elementos de celular e computador, ou puros, como os PDA's – *Personal Digital Assistant* –, que são unidades computacionais completas.

O uso de redes sociais para acesso de informação particular usando dispositivos móveis pessoais, durante o expediente de trabalho, dentro ou fora da organização não será abordado no presente trabalho.

Embora consumerização e BYOD estejam intrinsecamente relacionados ao conceito de *cloud* – navegação na nuvem –, ele não será tratado nesta obra, pois isto exigiria um aprofundamento muito grande. Não obstante, os termos c*loud* e nuvem serão usados com o mesmo significado e ambos irão aparecer ao longo de todo trabalho.

A consumerização é uma questão de gerenciamento de redes. Por se tratar de uma realidade nova, ela demandará soluções inovadoras da TI – setor de Tecnologia da Informação da empresa. Porém, também é possível utilizar, neste este novo problema, técnicas de gerenciamento tradicionais com adaptações.

Para se criar modos de lidar com a consumerização é preciso conhecê-la e este Trabalho de Conclusão de Curso pretende caracterizar o tema para que ele possa ser melhor compreendido e para que nele possam ser aplicados as melhores técnicas de gerenciamento.

Parece haver uma imensa quantidade de soluções dos administradores de TI, tanto no Brasil como no exterior, para o problema da consumerização. Este trabalho se esforçará para mostrar algumas de suas características principais e do programa BYOD, tais como propriedade, produtividade, suporte e segurança, que serão abordados nos Capítulos 3. No Capítulo 4, falaremos como o BYOD pode ser inserido na Política de Segurança da Informação das empresas, e mostraremos dois estudos de casos de implementações do mesmo.

As opiniões dos que trabalham com administração de redes corporativas e os estudos de institutos de pesquisa de nível mundial dizem que a consumerização é um movimento que vem para ficar. Sendo assim, e por ser um problema de infraestrutura de TI, presente das pequenas às grandes redes e até mesmo na espinha dorsal dos sistemas, ela merece ser estudada afim de melhor trabalhá-la.

Depois de firmada uma base teórica sólida para o tema, pode-se caminhar para o estabelecimento de melhores práticas que otimizem cada vez mais a relação de custo-benefício das empresas para com a consumerização.

2. CONSUMERIZAÇÃO

A consumerização é um fenômeno muito mais amplo do que somente a utilização de dispositivos móveis pessoais para trabalho. Neste capítulo, será demonstrado como várias forças da sociedade estão envolvidas ao mesmo tempo para a sua criação, tais como os próprios colaboradores, o mercado de consumo em massa e os desenvolvedores e fabricantes de tecnologia.

O próprio conceito de local de trabalho está modificando. A consumerização indica uma mudança na maneira como as pessoas trabalham e favorece o enfraquecimento dos limites entre nossa vida pessoal e profissional, e esta maior integração vem corresponder ao anseio de muitas pessoas nos dias de hoje.

É necessário analisar o aspecto social da consumerização para poder realizar qualquer planejamento estratégico nas empresas para gestão da tecnologia da informação. Em particular, a TI das organizações precisa compreender o significado deste movimento para poder gerenciar o programa BYOD.

2.1. Aspecto social da consumerização

O termo consumerização é o aportuguesamento da palavra *consumerization.* E esta por sua vez vem da raiz *consumer*, que significa consumidor em português. Quando se fala em consumerização do ambiente de trabalho, consumerização da TI etc., se está falando de uma ordem de coisas em que os recursos do ambiente de trabalho, os recursos da TI, entre outros, passam a ter um foco cada vez maior nas tecnologias disponíveis no mercado de consumo em massa, as quais são utilizadas pelos colaboradores.

Recentemente, as empresas norte-americanas estão recebendo muita influência, tanto em forma de concorrência do mercado, como dos próprios colaboradores, por uma mudança na cultura da organização. Além disso, conforme o

mercado de dispositivos móveis evolui, mais tecnologias são desenvolvidas para auxiliar a TI no gerenciamento dos mesmos, tornando mais simplificado a sua gestão no ambiente corporativo.

Devido a isso muitas pesquisas têm sido realizadas e artigos têm sido escritos sobre o tema. Este trabalho se baseia, em sua maior parte, em pesquisas realizadas no mercado norte-americano junto a empresas de todos os segmentos. Pode-se dizer que outras regiões centrais, tais como Europa, Japão, tigres asiáticos, China e outros, estão muito próximas da realidade norte-americana (IDC, 2013).

No Brasil, embora distante de uma popularização maior dos dispositivos móveis e de programas BYOD, pode-se dizer que estão começando a ser introduzidos nas grandes empresas pelo alto empresariado, e principalmente em empresas ligadas a tecnologia de ponta, seguindo os modelos norte-americanos.

Como diz Taurion (2013b), lutar contra este movimento é inútil e não agrega nenhum benefício para as empresas e, em sua opinião: “Em vez de construir uma inútil mureta contra o *tsunami* que está chegado, é mais inteligente entender o movimento de consumerização”.

Em 2007 foi lançado o *iPhone*, e, em 2010, o *iPad*. Apesar de não serem produtos inteiramente novos no mercado, foram o resultado de um projeto que obteve muitos cuidados da *Apple* – desenvolvedora de tecnologia – e foram conceitualmente novos, no sentido de oferecerem um pacote de funcionalidades multimídia e para *Web* que atendiam ao gosto popular. Ou seja, eles foram projetados para o consumo em massa.

Outros fabricantes ofereciam *hardware* e SO – Sistema Operacional – com qualidades bastante similares, mas o diferencial do produto foi a grande promoção publicitária feita pela *Apple* e seu então tutor, Steve Jobs. Mais do que promover seus produtos, o que eles fizeram foi tornar os produtos “*smartphone*” e “*tablet*” mais conhecidos, até mesmo a nível mundial.

Nos últimos anos o aumento do número de vendas deste tipo de dispositivos foi expressivo. Isto tem acarretado em consideráveis modificações nas empresas

modernas, como podemos ver em artigos e pesquisas realizadas, em grande quantidade, entre profissionais de empresas norte-americanas.

Com a popularização dos dispositivos móveis em geral, acelerada pela grande publicidade dos produtos específicos da *Apple*, os dispositivos móveis passaram a integrar e administrar cada vez mais a vida pessoal e a naturalmente fazer parte do ambiente de trabalho. Nos últimos anos temos observado cada vez mais ao fenômeno da consumerização dos ambientes de trabalho (GILBERT; GREENGARD, 2013b).

Trata-se de um fenômeno que não tem data de início certa e pode ser inserido num movimento de inovação tecnológica anterior e mais abrangente. Conforme informa Moschella (2013), em um importante trabalho de pesquisa de 2004 desenvolvido pela CSC – *Computer Sciences Corporation* –, empresa mundial de desenvolvimento de soluções em TI, nos EUA a inovação tecnológica entre as décadas de 60 e 80, seguiu o modelo *top-down* – de cima para baixo – estimulada principalmente pelos gastos com pesquisa das forças armadas norte-americanas e pelo incentivo da iniciativa privada para produzir P&D – Pesquisa e Desenvolvimento.

As forças armadas recebiam altos volumes de investimento do governo, devido principalmente ao pós-guerras e à disputa entre a ex-União Soviética e os EUA para a chamada “conquista da lua”, que elevou o nível de investimento em pesquisa nos EUA de forma vultuosa.

Por outro lado, com a parceira entre governo norte-americano, universidades e iniciativa privada para produzir P&D, aos poucos os novos conhecimentos tecnológicos adquiridos foram sendo transmitidos para as grandes empresas seguindo este modelo *top-down* de inovação tecnológica. E aos poucos também para as empresas de menor porte.

Conforme diz Moschella, a partir da década de 80, e coincidindo com a criação do computador pessoal, ou PC – *Personal Computer* – pela IBM e *Microsoft*, este modelo começou a sofrer a pressão de outra fonte de inovação, que seguia o modelo *bottom-up* – de baixo para cima –, quando os conhecimentos tecnológicos

adquiridos no modelo *top-down* foram aplicados na indústria voltada para o mercado de consumo em massa.

Portanto a consumerização representa a mudança na lógica do modelo *top-down* de inovação tecnológica. O surgimento do PC é representativo de uma época onde as tecnologias disponíveis no mercado consumidor, ou seja, que podiam ser adquiridas por qualquer pessoa, levadas para suas casas e se tornar de uso pessoal, passam a se igualar e a superar em poder computacional as tecnologias utilizadas pelas empresas.

Estas tecnologias pessoais são utilizadas no ambiente de trabalho em volume cada vez maior, e, então, o ritmo de inovação destas tecnologias voltadas para o mercado de consumo em massa passa a ser muito mais expressivo que o da tecnologia utilizada pelas grandes empresas (MOSCHELLA, 2013).

May (2013), em trabalho recente, diz que esta mudança não chega sem provocar tensão. Segundo ele, existe uma dessincronização entre o modelo antigo, em que toda a infraestrutura da empresa é de propriedade da organização e gestão exclusiva da TI, e o novo modelo, onde as maiores inovações estão acontecendo, que é aquele fomentado pelo mercado de consumo em massa.

Para ele, essa tensão ocorre porque as mudanças fora da empresa estão acontecendo num ritmo muito mais veloz do que as mudanças dentro da empresa.

2.2. Consumerização como tecnologia disruptiva

A teoria disruptiva e os casos de inovações disruptivas, foram estudados pelo pesquisador norte-americano Clayton Christensen, autor da obra *The Innovator's Dilemma: when new Technologies cause great firms to fail*, a qual analisou e modelou este tipo de fenômeno em 1997, e sua posterior continuação em 2003, *The Innovator's Solution: creating and sustaining successful growth*, ambos publicados pela Harvard Business School Press de Boston.

Segundo Moschella (2013), as organizações necessitam entender a teoria disruptiva e como ela pode afetar suas operações. Christensen diz que as organizações podem reagir à inovação de maneiras racionais, porém, que a longo prazo podem ter conseqüências severas. Para Moschella, a consumerização é um típico caso do que é tratado academicamente como tecnologia disruptiva, com o que concordam outros autores como Ackerman e Guzzo (2013) e Gilbert (2013).

Um caso de tecnologia disruptiva teria sido o PC, criado na década de 80 pela *Microsoft*. Houve casos de empresas que, pouco antes da inovação provocada pela criação da *Microsoft,* investiram em outras plataformas. A força que os PC's rapidamente obtiveram no mercado consumidor impôs um fracasso comercial a estas empresas, que não conseguiram se adaptar à tendência imposta por esta tecnologia disruptiva a tempo.

O comportamento das tecnologias disruptivas, como mostram outras situações analisadas por Christensen, pode ser comparado a um gráfico com duas retas com ângulos de inclinação positivos e diferentes entre si, onde uma representa a temporalidade da inovação das tradicionais infraestruturas e sistemas de negócio, e outra a temporalidade da inovação de tecnologias disruptivas, a qual, por ser mais veloz, tem inclinação mais acentuada.

Conforme se pode ver na figura 1, e baseando-se em Moschella, a reta com maior inclinação, e que, portanto, progride num ritmo mais veloz que a outra, é aquela que representa a inovação no modelo *bottom-up*, e a reta com menor inclinação, é aquela que representa a inovação no modelo *top-down*, o qual é mais resistente a mudanças, e, portanto, tem a sua inovação implementada num ritmo mais lento.

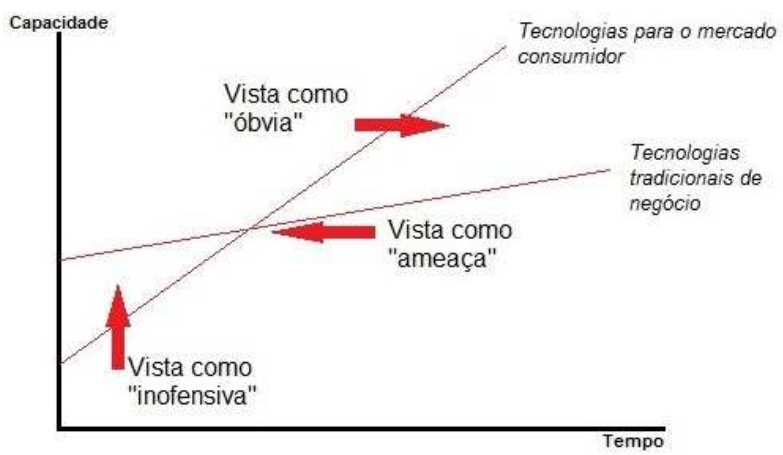

Figura 1: Consumerização como tecnologia disruptiva (AUTORIA PRÓPRIA, 2013).

Como diz Moschella (2013), quando uma tecnologia disruptiva aparece, geralmente ela possui muitas deficiências e carências, como, por exemplo, performance, confiabilidade e segurança, entre outros, as quais as tornam inapropriadas para as grandes organizações.

A adoção desta tecnologia, a princípio, se dá por poucos envolvidos com a organização (como aqueles colaboradores mais aficcionados). Inicialmente, portanto, a infraestrutura tradicional da empresa não sofre nenhum impacto significativo, e, assim, muitas vezes, a tecnologia inovadora é esquecida ou mesmo ignorada, sendo a fase que ela é vista como inofensiva.

Porém, conforme a nova tecnologia imprime um ritmo de inovação mais veloz que o das tecnologias tradicionalmente utilizadas na empresa, aquela vai, eventualmente, se equiparar em capacidade com esta estrutura antiga, sendo a fase em que ela é considerada como ameaça. Posteriormente, irá ultrapassá-la em termos de capacidade e eficiência de trabalho, sendo a fase em que ela é considerada como óbvia, ou comum.

Moschella (2013) ressalta que o senso comum imagina que as mudanças na área tecnológica ocorrem de forma mais veloz do que realmente ocorrem. Mas para ele, pode levar anos para que seus principais efeitos se tornem aparentes. Porém, claramente, aquelas empresas que têm o poder de aumentar o seu controle sobre o

movimento de consumerização, estão em condição de passar por essa transição de forma mais tranqüila.

Para ele, em artigo, como mencionado, de 2004, e falando sobre a realidade norte-americana, as evidências sugeriam fortemente que a intensa força inovadora das tecnologias disponíveis para consumo em massa havia passado do primeiro estágio, para o segundo, se mostrando cada vez mais como uma ameaça para as organizações, considerando que sua base de utilização era grande e estava em crescimento, e que o futuro tecnológico já dava sinais de estar assegurado pra essas tecnologias, muitas das quais já possuíam um forte amadurecimento no mercado.

2.3. Conformidade

Um dos aspectos mais importantes da consumerização é com relação à conformidade. Define-se conformidade como o fato de uma organização estar em acordo com as normas que são previamente por ela mesma estabelecida. Em países como os EUA, a preocupação com a conformidade é muito grande, além de uma exigência, por exemplo, de investidores e acionistas, e um fator de diferencial comercial das empresas.

Como foi visto, a força da inovação das tecnologias disponíveis para consumo em massa dentro do ambiente de trabalho é muito grande e as empresas sentem pressão para estar alinhadas com este movimento, que se torna cada vez mais generalizado. Realizar isto de dentro dos limites de conformidade e segurança é um dos desafios das organizações.

Na opinião de uma interessante pesquisa sobre consumerização da TI realizada em 2011 pela empresa *Proofpoint*, que desenvolve soluções em segurança da informação, o maior risco para as empresas é não acompanhar este movimento. Independentemente de qualquer medida da organização, os

colaboradores em geral estão usando dispositivos móveis pessoais dentro do ambiente de trabalho (PROOFPOINT, 2013).

A política de segurança da empresa não está sendo seguida, devido à força inovadora do modelo *bottom-up*, ou seja, da invasão de tecnologias do mercado consumidor no ambiente de trabalho. Segundo a pesquisa, apesar de muitas empresas terem normas de segurança e conformidade bem desenvolvidas, os colaboradores não as estão seguindo.

Grande parte, ou, virtualmente toda a comunicação interna, está sendo realizada fora da esfera de controle da empresa e, portanto, tentar controlar rigidamente ou mesmo impedir o movimento de consumerização é um risco para a empresa, que pode se ver com problemas para assegurar questões de conformidade.

Para as organizações, é fundamental retomar o controle sobre a consumerização, e o modo sugerido pela *Proofpoint* (2013) é um modelo de solução baseado em confiança no colaborador, na implementação de uma política de segurança da informação que abranja os dispositivos móveis e no uso de tecnologias para gerenciamento de dispositivos móveis e segurança da empresa

2.4. Aspecto comercial do BYOD

Como foi visto, a consumerização possui um aspecto social, podendo ser caracterizada como uma inovação tecnológica com algumas conseqüências sociais.

O BYOD é um fenômeno mundial. Observando-se a base de celulares no mercado mundial em números absolutos, vê-se que 70% da população mundial tem um celular. Por outro lado, a proporção de *smartphones* com relação ao total de telefones vendidos cresce cada vez mais. Atualmente, nos EUA, 80% dos telefones vendidos são *smartphones*, já no caso do Brasil, 44% (FORBES; FOLHA; TELECO, 2013).

Nos EUA, a quantidade de pessoas que possuem *smartphones* ultrapassou a de pessoas que possuem celulares. No Brasil, a proporção de *smartphones* com relação ao total de telefones celulares é de aproximadamente 7%. Vê-se que em números absolutos a quantidade de *smartphones* no Brasil ainda é pequena, num país cuja realidade social é radicalmente diferente da norte-americana (MOREIRA; LOBO, 2013).

Todavia, o seu uso para acesso à Internet é expressivo, sendo que, atualmente, mais de 30%, ou quase um terço da população brasileira, acessa a Internet utilizando dispositivos móveis, o que representa um prognóstico muito positivo para o futuro destes aparelhos no Brasil (SCRIVANO, 2013).

Comparando-se as realidades brasileira e norte-americana percebe-se por que o BYOD já possui expressividade nos EUA e tende a aumentar muito mais, enquanto no Brasil tem somente tímidas expressões.

Além disso, ao menos no que tange à realidade norte-americana, o índice de utilização de dispositivos móveis pessoais pelos colaboradores no trabalho é muito grande. Para a empresa desenvolvedora de tecnologia *TrackVia*, 80% dos colaboradores utilizam tecnologia pessoal para trabalho. Na opinião da Avanade, empresa que provê serviços de TI focados em *Windows* para médias e grandes empresas, o índice é ainda maior: 88% (TRACKVIA; AVANADE, 2013).

Os dispositivos móveis, segundo Greengard, já são os que mais acessam as grandes redes sociais, e ainda no ano de 2013 devem ultrapassar os PC’s como os dispositivos que mais acessam a *Web* (GREENGARD, 2013b).

Quanto mais dispositivos há no ambiente de trabalho, mais as empresas se movem para desenvolver políticas de segurança. A Avanade, em uma pesquisa em 2012 junto a 605 executivos e profissionais de TI em 17 países, constatou que as empresas estão aderindo à consumerização.

Para 73% das empresas, o tema BYOD possui alta prioridade em suas organizações. E a maioria das empresas, 60%, estão em processo de adaptação de suas infraestruturas de TI para poder suportar os dispositivos pessoais dos colaboradores.

A pesquisa *Mobility Temperature Check: Just How Hot is BYOD?*, realizada em 2012 pela CCMI, empresa norte-americana líder em pesquisa sobre taxas e tarifas da indústria de telecomunicações, junto a 116 profissionais de TI e do setor de telecomunicações de renome nos EUA, chegou a números parecidos com os da Avanade (CCMI, 2013).

A princípio, o BYOD não tem sido visto como fator direto de competitividade pelas empresas. Segundo a pesquisa da CCMI, apenas 9% das empresas acham que precisam aderir ao BYOD para competir com concorrentes.

Porém, indiretamente, pode-se dizer isso, pois ele é visto com um fator que agrega valor à imagem da empresa. Para Moschella, aderir à consumerização pode trazer ganhos em imagem e liderança no mercado frente a outras empresas.

Por outro lado, a CIO Brasil diz que as empresas que não implementam BYOD estão perdendo colaboradores, principalmente os mais jovens e criativos, para as que o fazem. O BYOD está sendo utilizado para atrair novos recursos humanos, agregando competitividade no mercado (CIO, 2013c).

Outra questão comercial importante, relativa à imagem da empresa, é com relação aos riscos envolvidos com BYOD. Segundo a pesquisa da Avanade, a segurança da informação é vista como o fator de maior risco para os programas BYOD para 66% das empresas.

Não obstante, enquanto muitos consideram a consumerização difícil de ser integrada no ambiente de trabalho e cheia de riscos, aquelas empresas que têm sucesso em gerenciar a integração com o BYOD e manter as especificações relativas à conformidade podem criar uma imagem sólida e de liderança no mercado (CIO, 2013d; MOSCHELLA, 2013).

Percebe-se, portanto, que, apesar do programa BYOD não ser visto como fator direto de competitividade entre os executivos, indiretamente ele tem grande influência neste fator comercial. Esta influência se dá de duas formas: primeiramente perante a certificação com relação a normas de conformidade mencionada no capítulo anterior, valorizada perante o mercado, e, em segundo lugar, através da

imagem de modernidade relativa à gestão dos recursos humanos transmitida ao mercado.

2.5. Papel da TI

No primeiro capítulo do artigo da *Microsoft* publicado em 2011, *Strategies for Embracing Consumerization*, lê-se que o conceito de ambiente de trabalho está mudando. Segundo Moschella, a fim de melhor acompanhar a consumerização, as organizações devem entender que cada vez mais há uma mescla do ambiente pessoal com o ambiente de trabalho (MICROSOFT; MOSCHELLA, 2013).

A consumerização oferece novas formas de personalização no trabalho: utilização da *Web* para o trabalho; opções de não utilizar serviços corporativos para tarefas de trabalho; utilização de *softwares* livres, sistemas operacionais alternativos ou mesmo ferramentas desenvolvidas pelo próprio colaborador; opção de utilizar serviços de *e-mail* da *Web* e não o *e-mail* próprio da empresa; opção de utilizar outros meios para comunicação no trabalho, como mensageiros instantâneos ou redes sociais etc (GREENGARD, 2013b).

Em um artigo da desenvolvedora de tecnologia *Intel*, a respeito da visão do local de trabalho do futuro, vê-se que a flexibilidade de local e horário de trabalho será fator mais importante na escolha da empresa na qual trabalhar do que o salário. Além disso, alguns conceitos estão se modificando, como o de lealdade dos colaboradores com relação à empresa em que trabalham. Segundo o artigo, as pessoas não se sentem ligadas a um lugar, só permanecendo enquanto lhes é vantajoso.

Um outra mudança é que o conceito de escritório esta se tornando algo menos rígido, menos imprescindível para a realização do trabalho, abrindo a possibilidade para, por exemplo, se realizar tarefas de trabalho em casa, ou mesmo, ficar a maior parte da semana trabalhando em casa (MAISTO; MICROSOFT, 2013)

Ao mesmo tempo, como diz a pesquisa da Avanade, a consumerização oferece potencial para gerar vantagens pra a organização, tais como gerar inovações na maneira como os colaboradores trabalham e acessam serviços da empresa, além de entregar mais flexibilidade para o colaborador gerenciar seu próprio ritmo de trabalho.

Atualmente, as tecnologias disponíveis para o mercado consumidor podem ser superiores às utilizadas no ambiente de trabalho, em termos de desempenho computacional. Além disso, os colaboradores, principalmente os mais jovens, estão se tornando cada vez mais experientes com seus aparelhos, sabendo utilizá-los da forma mais eficiente para seu próprio trabalho, e assim, estimulando a produtividade (CCMI, 2013).

Portanto, a atitude exigida para a TI diante da consumerização é de pró-atividade, com o momento exigindo uma antevisão de acontecimentos. Segundo Moschella (2013), a postura da TI diante, de um lado, da força inovadora da consumerização, e de outro, da infraestrutura arcaica de negócios da organização, deve ser de promover inovação, liderança e integração, promover a imagem da empresa e a transição entre os modelos.

A pesquisa do IDC – *International Data Corporation* – de 2012, intitulada *IT Decision Makers Feeling the Pressure to Adopt Bring-Your-Own-Device Strategies*, mostra que a TI está sentindo a pressão para conseguir integrar o modelo *top-down*, levado a cabo pelos executivos da empresa, com a demanda do modelo *bottom-up*, dos colaboradores em geral, pelo uso de dispositivos móveis no ambiente organizacional (IDC, 2013).

Segundo Moschella (2013), as organizações precisam repensar cuidadosamente suas políticas de segurança. Uma revisão geral das suas diretrizes e procedimentos deve ser realizada, e, no momento este é um dos papéis que cabe à TI, e ele deve ser realizado com uma atitude realmente pró-ativa e inovadora.

Como diz May (2013), nós estamos cinco décadas adentro da era da informação e ainda usamos modelos de trabalho e organização da era industrial. A

TI, outrora, no modelo *top-down* de inovação tecnológica, tinha o controle do *hardware* e *software*, físico e lógico, da infraestrutura da empresa.

Conforme a consumerização vai ganhando força, cada vez mais a TI vai perdendo este controle absoluto do seu ambiente, exigindo uma mudança nesta dinâmica. Ela está forçando as empresas a repensar a relação de seus colaboradores com seus recursos e informação.

Isto implica em adotar um modelo de abordagem diferenciado, com relação ao colaborador, não mais baseado na antiga relação paternalista mantida pela TI para com os colaboradores, mas devendo enxergá-los como clientes, estimulando a responsabilidade e o poder de escolha.

Como diz a Avanade (2013), a TI deve sair da posição de rígidos controladores do uso de dispositivos móveis na empresa, para promovedores destes dispositivos, aplicativos e serviços. As organizações devem transformar o papel da TI de uma função reativa e mitigadora de riscos, para gestores estratégicos que alavancam o potencial desta inovação tecnológica para benefício de suas empresas.

Para realizar esta transição de forma segura, é conveniente citar o portal brasileiro da revista CIO – *Chief Information Officer* – hospedado pela UOL – Universo *On-Line* –, que é da mesma opinião que a pesquisa da empresa *Proofpoint* ao dizer que o modelo para garantir a adequação da BYOD com relação à conformidade e segurança da informação deve ser baseado na gestão moderna dos colaboradores, na implementação de uma política de segurança da informação que abranja também dispositivos móveis e no uso de tecnologias para gerenciamento de dispositivos móveis (CIO, 2013b; PROOFPOINT, 2013).

Desta opinião também é Sêmola (2003), ao afirmar que só uma gestão estratégica destes três níveis é o que pode realmente assegurar a proteção da segurança da informação. O próximo capítulo analisará como concretizar isto no programa BYOD das empresas.

3. PROGRAMA *BRING YOUR OWN DEVICE* – BYOD

Pode-se definir o programa BYOD como a política de segurança da informação da empresa com relação aos dispositivos móveis utilizados por seus colaboradores para fins de trabalho.

O programa BYOD, em algumas fontes, foi também referenciado como BYOT – *Bring Your Own Technology*. Assim como outro termo, o BYOC – *Bring Your Own Cloud* –, ou mesmo BYOx – *Bring Your Own X* – são conceitos que acarretam em algumas diferenças, mais ou menos sutis, para com BYOD, porém, neste trabalho, não se fará diferenciação entre eles. Para todos os efeitos, será considerado somente o BYOD (CIO, 2013b; TAURION, 2013a, 2013b).

Como foi visto, muitas empresas já iniciaram seus programas BYOD, e há uma grande quantidade de programas implementados e em funcionamento. Cada programa é único, e deve estar de acordo com a natureza da organização. Não obstante, neste capítulo serão vistas algumas características que podem ser encontradas em todos os programas BYOD. Antes, porém, serão feitas algumas definições.

A pesquisa da CMMI, em sua metodologia, define como Baseado na Empresa (*Corporate-Liable*), ou BE, o modelo de gestão de dispositivos móveis em que a organização adquire, gerencia e protege todos os dispositivos, pagando todas as contas mensais de planos de serviço.

Baseado no Colaborador (*Employee-Liable*), também referenciado pela pesquisa como BYOD puro, o modelo no qual os colaboradores adquirem os dispositivos, usam-nos no ambiente de trabalho e são responsáveis por pagar as contas mensais de planos de serviço. A pesquisa diz que algumas empresas optam por reembolsar os colaboradores pelo uso relacionado com o trabalho, como veremos posteriormente.

O modelo híbrido é uma mistura dos modelos Baseado na Empresa (BE) e Baseado no Colaborador (BC), e é o modelo que tende a ser o mais utilizado,

correspondendo, na prática, ao programa BYOD. As empresas estão buscando ferramentas para adquirir, gerenciar e proteger todos os dispositivos, para que possam ser controlados pela da TI independente de quem compra o aparelho (CCMI, 2013).

Neste capítulo também serão utilizados os conceitos de *capex* e *opex*. *Capex* vem da expressão *capital expenses*, ou seja, despesas com capital. Ele está relacionado com a aquisição de novos equipamentos ou substituição de equipamentos.

Já *opex*, vem de *operational expenses*, ou seja, despesas operacionais. Está relacionado à manutenção de equipamentos já em funcionamento na empresa, ou seja, está ligado a despesas com suporte.

Estes termos, *capex* e *opex*, se referem aos gastos da empresa relacionados somente com dispositivos móveis, separadamente dos gastos com o restante da infraestrutura de TI da empresa. Busca-se com isso avaliar efetivamente o quanto o programa BYOD agregou ou onerou à organização.

3.1. Propriedade

A questão da propriedade é uma das que mais embaraça a evolução do programa BYOD. John Pironti, presidente da empresa de consultoria *IP Architects,* que assessorou questões de segurança sobre BYOD na ISACA, associação profissional internacional de governança em TI, diz que as questões jurídicas são mais difíceis de responder do que as de tecnologia (COMPUTERWORLD, 2013a).

Pelo fato do BYOD agregar competitividade no mercado, muitas empresas possuem óbvias preocupações com relação a questões trabalhistas relativas à propriedade dos dispositivos móveis, tais como possíveis pedidos de indenização.

Acurou-se na pesquisa *Mobility Temperature Check: Just How Hot is BYOD?*, realizada pela CCMI, que os três maiores objetivos dos programas BYOD são

manter os colaboradores motivados, aumentar a produtividade e reduzir despesas (CCMI, 2013).

Porém, os dois primeiros objetivos são difíceis de medir em termos quantitativos e, como será visto mais adiante, ainda não há garantias de que realmente ocorrem. Ora, se o terceiro é diminuir as despesas, então todos os pontos de um programa BYOD devem ser voltados para este objetivo.

Uma das maiores fontes de despesas de um programa BYOD são os relativos a manobras do departamento de recursos humanos para proteger a empresa de questões jurídicas com relação à propriedade dos aparelhos que a implementação do programa acarreta.

Para entender uma possível raiz deste problema, é importante observar a recente Lei Federal Nº 12.551, de 2011, que altera o Artigo 6º do Decreto-Lei Nº 5.452 da Presidência da República, de 1º de maio de 1943, o tão conhecido decreto que aprova a CLT – Consolidação das Leis do Trabalho:

> "Art. 6º. Não se distingue entre o trabalho realizado no estabelecimento do empregador, o executado no domicílio do empregado e o realizado a distância, desde que estejam caracterizados os pressupostos da relação de emprego.
>
> Parágrafo único. Os meios telemáticos e informatizados de comando, controle e supervisão se equiparam, para fins de subordinação jurídica, aos meios pessoais e diretos de comando, controle e supervisão do trabalho alheio" (PALÁCIO, 2013).

A Lei Federal Nº 12.551, de 15 de dezembro de 2011, é uma alteração recente do Artigo 6º da CLT, porém, não favorece ao programa BYOD ao definir, em seu único parágrafo, que os meios telemáticos – ou seja, de comunicação à distância – utilizados para trabalho se equiparam ao restante dos equipamentos de propriedade empresa.

Assim, de acordo com a legislação brasileira, é possível interpretar-se que o uso do dispositivo móvel pessoal pelo colaborador deve ser indenizado pela organização. Portanto, para que os programas BYOD possam ganhar maior sucesso, seria necessário uma outra alteração no texto da legislação, adequando-o à nova realidade social.

Segundo Patrícia Pinheiro, advogada especialista em Direito Digital, citada pela revista CIO Brasil, um dos primeiros pontos a ser definido durante o planejamento do programa BYOD é deixar muito bem definido de quem é a propriedade dos dispositivos (CIO, 2013a).

Ressalta-se que a utilização de *notebooks*, celulares, *smartphones,* PDA's etc., pessoais ou não, pelos colaboradores para fins de trabalho, desde há muitos anos não é novidade. Porém, isto ocorria com menos freqüência, e geralmente era reservado este benefício ou privilégio a colaboradores com funções elevadas ou específicas dentro da organização.

A consumerização é um movimento que segue o modelo *bottom-up* de inovação tecnológica e pressiona a favor da utilização cada vez mais generalizada, pelos colaboradores, de tecnologia disponível no mercado de consumo em massa. As organizações precisam criar meios para viabilizar isso sem terem que arcar com o ônus para a permissão que dá ao colaborador para utilizar seu dispositivo pessoal para trabalhar na organização.

Uma forma para isso é criar mecanismos dentro da política de segurança, que possuam a concordância do colaborador a respeito de determinadas definições. A pesquisa da CCMI mostra que 52% das empresas que possuem políticas de segurança implementadas recorrem ao artifício de pedir que os colaboradores concordem por escrito com determinações como parte da estratégia de gestão do programa.

Como a TI não possui mais o controle total dos dispositivos que compõem a infraestrutura da organização, não se pode garantir sem sombra de dúvidas que não haverá mal uso ou uso com má fé dos dispositivos por parte de seus colaboradores, e, assim, sofrer embaraços jurídicos como, por exemplo, o concernente de quem é a

responsabilidade por *softwares* e aplicativos proprietários instalados no dispositivo móvel sem possuir a devida licença.

Como forma de proteger a empresa, a TI deve fazer com que os colaboradores concordem por escrito com normas que possuam um alto grau de detalhamento. Quanto mais detalhado estiverem estas definições na política de segurança, maior o grau de proteção jurídica oferecido para a empresa.

Por outro lado, a empresa precisa monitorar os dispositivos móveis pessoais dos colaboradores que utilizam seus recursos de TI. Eventualmente ela poderá se julgar no direito de rodar um aplicativo de segurança, analisar trilhas de auditoria ou mesmo deletar arquivos com informação corporativa. Como tais ações, mesmo com a utilização de *software* automatizado de gerenciamento, envolvem também a ação humana, erros podem ser cometidos, como, por exemplo, a exclusão acidental de arquivos pessoais do colaborador.

Devido a tais medidas acarretarem em um óbvio risco de causar constrangimento para o colaborador, a empresa precisa utilizar do mecanismo de fazer com que o colaborador esteja ciente e de acordo com o monitoramento de seu dispositivo pela empresa, a fim de proteger a organização de possíveis pedidos de indenização,

Outra solução para o problema da propriedade dos dispositivos móveis é separar o máximo possível os ambientes pessoal e de trabalho logicamente. As primeiras soluções neste campo utilizavam largamente um forte esquema de controle de acesso baseado em autenticação com criptografia dos dados transmitidos. Então em cima desta base foram aplicadas soluções de VPN's – conexões privadas seguras.

Atualmente, manteve-se essa base onde todos os acessos e transmissões de dados se baseiam em autenticação com criptografia, e estão sendo utilizadas técnicas de virtualização para isolar, em um mesmo aparelho, os ambientes pessoal e profissional, permitindo o compartilhamento de acesso a aplicações e arquivos. Neste campo, algumas empresas estão conseguindo inclusive realizar a segurança e o gerenciamento de usuários e não mais de dispositivos.

Outro fato de destaque é que os fabricantes de tecnologia estão direcionando seus produtos para oferecer uma solução a nível de *hardware*, para facilitar o trabalho da TI em gerenciar estes dispositivos móveis. Um exemplo neste campo é o *Dual Persona*, desenvolvido pela empresa espanhola *Telefônica*, o qual permite ao usuário contar com duas linhas em um mesmo aparelho, a pessoal e a corporativa. Também a nível de *software*, várias funcionalidades que atendem a necessidades da TI, estão sendo desenvolvidas pelos fabricantes com a mesma finalidade (COMPUTERWORLD, 2013c).

A separação entre estes dois ambientes pode, inclusive, ser fundamental para se alcançar os níveis de conformidade exigido pela empresa. Esta separação lógica também pode resolver os problemas com relação ao constrangimento causado para o colaborador ao ter seu dispositivo monitorado.

Como parte da gestão da propriedade dos dispositivos móveis do programa BYOD, as empresas precisam definir qual modelo seguirão. Segundo a pesquisa da CCMI, 60% das empresas entrevistadas mantêm um modelo BE de gerenciamento de dispositivos móveis, pagando todas as despesas com telefones e contas mensais de planos de serviço. O modelo híbrido é implementado por 22% das empresas. E 10% mantêm um modelo BC ou BYOD puro, e esperam que os colaboradores arquem integralmente com as despesas mensais.

O modelo híbrido, no entanto, está crescendo cada vez mais, e muitas empresas que possuem modelo BE pensam em fazer a transição pra o híbrido. Entre estas, é comum o planejamento das formas como ocorrerão o reembolso do colaborador. Para a pesquisa, há dois métodos principais para reembolso: mediante apresentação de relatório de despesas e pagamento de estipêndio ou indenização mensal.

Os dois são exatamente opostos um ao outro. O estipêndio ou indenização mensal representa um valor que pode ser projetado e orçamentado, e, uma vez implementado, requer pouca administração. Trabalha, porém, com valores estimados. A apresentação de relatório é bem mais difícil de ser administrada, porém, representa o valor real gasto. Para muitas empresas é difícil trabalhar com

esta opção, pois estipular o orçamento para cima elimina o potencial do programa BYOD de reduzir gastos, e para baixo, deixa os colaboradores insatisfeitos.

Outro método empregado é a transferência legal do dispositivos, a qual, algumas vezes pode ser definitiva. No caso da não definitiva, que tende a ser o método mais utilizado, recebe o nome de *comodato*.

O *comodato* é um mecanismo jurídico no qual o colaborador adquire o dispositivo móvel, e posteriormente vende para a organização por uma quantia simbólica (que não necessariamente é o valor pago pelo colaborador). Esta se compromete a vender o dispositivo para o colaborador pela mesma quantia quando ocorrer seu desligamento da empresa, (CIO, 2013d).

Portanto, apesar da questão relacionada à propriedade dos dispositivos provavelmente só poder ser solucionada definitivamente após modificação no próprio texto da legislação trabalhista brasileira, percebe-se que as empresas primeiro precisam definir suas estratégias de gestão da propriedade dos dispositivos, e então implementarem tecnologias de gerenciamento que a auxiliem a separar o máximo possível os ambientes pessoal e profissional. A técnica de concordância por escrito também será de especial ajuda nesta questão.

Assim, espera-se diminuir as despesas da empresa com questões trabalhistas, que, no caso de empresas médias ou pequenas, podem ser o suficiente para causar dificuldades financeiras. Outra finalidade é diminuir o desperdício de recursos das empresas com relação a orçamentos anuais mal projetados.

3.2. Produtividade

Como já foi mencionado, os três maiores objetivos dos programas BYOD são manter os colaboradores motivados, aumentar a produtividade e reduzir despesas segundo pesquisa da CCMI (2013). Este capítulo abordará os dois primeiros, os quais se espera melhorar com a implementação do programa BYOD. Este capítulo

também será utilizado para argumentar a respeito da lucratividade ou não do programa.

A pesquisa da CCMI mostra que o motivo principal, com 19%, para os executivos implementarem o programa BYOD nas suas empresas, é o desejo de criar uma cultura corporativa amigável, seguido pela crença de que a produtividade do colaborador pode aumentar, com 17%, e pela esperança em reduzir as despesas da organização com dispositivos móveis, com 15%.

Isso mostra que o aumento da produtividade é uma verdadeira crença entre o empresariado, apesar de não haver ainda nenhuma pesquisa que confirme se há ganhos reais, de fato. O que existe é uma noção de que o programa BYOD pode melhorar a cultura interna da empresa, satisfazendo os anseios dos colaboradores e deixando-a mais em sintonia com os movimentos inovadores do mundo atual.

Por outro lado, não se pode esquecer de que é uma crança baseada na larga experiência e contato diário de profissionais da TI com os colaboradores. Henrique Sei, diretor de vendas de soluções da *Dell* Brasil, diz que:

> “A nova força de trabalho, na maioria jovem, puxou a demanda por dispositivos móveis pessoais na empresa. O movimento tem ainda papel de retenção de talentos, porque promove satisfação e produtividade” (COMPUTERWORLD, 2013c).

A consumerização, teoricamente, traz uma interação e, por conseguinte, um equilíbrio maior entre a vida pessoal e profissional. Na velocidade dos dias atuais, em que todos têm tantos afazeres e a impressão é de que há tão pouco tempo para conseguir dar cabo de todos os compromissos, a força inovadora da consumerização no ambiente de trabalho permite uma conciliação maior entre tantas atividades, em tantas áreas diferentes da vida, com tão pouco tempo disponível.

Mike Cunningham, diretor de tecnolgia da *Kraft Foods*, diz que o ganho mais relevante do programa BYOD da sua empresa está relacionado ao fato das pessoas

terem se tornado mais produtivas e terem melhorado a relação entre sua vida pessoal e profissional. Além disso, segundo ele, uma conseqüência indireta do programa BYOD foi que os colaboradores passaram a descobrir novas ferramentas para tornar o trabalho mais produtivo, e as quais a TI ignorava.

Leslie Jones, profissional de TI da *Motorola Solutions,* falando a respeito dessa esperança de que a motivação dos colaboradores aumente, diz que o programa BYOD pode elevar o moral, sendo um reconhecimento da demanda crescente de colaboradores para que usem a tecnologia que mais gostam.

A pesquisa da Avanade mostra como para a maioria dos executivos, 58%, o maior resultado do programa BYOD é o fato de que os funcionários podiam trabalhar de qualquer lugar que quisesse. 42% destes executivos relataram também que seus colaboradores estavam mais dispostos a trabalhar fora do horário de expediente (AVANADE, 2013).

Moschella (2013) diz que as tecnologias, infraestrutura e aplicações da consumerização poderiam trazer dramáticas diminuições de custos e melhorias igualmente significantes em funcionalidade do negócio e facilidade de uso. A pesquisa da *Proofpoint* (2013) também enxerga dessa maneira, quando diz que a adoção da consumerização da TI trouxe para as organizações aumento de eficiência e produtividade.

Em função deste objetivo, os orçamentos das empresas foram redefinidos com as despesas com dispositivos móveis, e pode-se considerar que há uma generosa alocação de recursos financeiros para o programa BYOD. Segundo a Avanade, em geral, 25% do total do orçamento com TI são reservados para gerenciar algum aspecto da consumerização.

A pesquisa conduzida pela CCMI (2013) relata que outras pesquisas recentes ainda não chegaram a uma resposta definitiva se os objetivos principais do programa BYOD objetivos estão sendo alcançados ou não. Já Borg (2013) diz que, apesar da crença inicial de muitas organizações de que o BYOD iria diminuir suas despesas com dispositivos móveis, um olhar mais de perto revelou que há despesas

ocultas que absorvem mais capital do que o aumento da produtividade dos colaboradores pode gerar.

Como exemplo, ele cita um pesquisa de 2011 do *Aberdeen Group*, que realiza análises de mercado, intitulada *Wireless Expense Management: Control International Roaming and the BYOD Revolution*, junto a 119 pequenas a grandes empresas de vários países, a qual mostra que uma companhia que adota o modelo híbrido de programa BYOD, com mais de 1.000 dispositivos móveis integrantes, dá um custo médio de 170.000 dólares a mais por ano do que uma organização baseada no modelo *top-down*, ou BE.

A Avanade também contesta um pouco a visão generalizada de que a consumerização traz motivação e produtividade, dizendo que para somente 32% dos executivos, o motivo principal pelo qual implementaram o programa BYOD em suas empresas foi o de tornar o local de trabalho mais atraente para os funcionários mais jovens. Para uma quantidade ainda menos expressiva, 20%, o programa beneficia novas contratações e retenção de talentos.

Para a pesquisa da CCMI, pouco foi alterado para as empresas com relação às despesas com dispositivos móveis, todavia, foram notadas algumas situações de aumento destas despesas.

De acordo com Kim Nash, da CIO dos EUA, citando uma pesquisa exclusiva da revista com 476 líderes da área de TI, ainda há muitas dúvidas sobre se o programa BYOD traz realmente economia de custos. Segundo esta pesquisa, 31% das empresas afirmam ter registrado economia com *capex* e *opex*, porém, a maioria, 43% não relatam qualquer economia de custos.

Na pesquisa da CCMI, vê-se que 66% das empresas que implementaram o programa BYOD disseram que não tiveram seus custos com *capex* reduzido, e 24% disseram que, na verdade, suas despesas com *capex* aumentaram mais de 20%. Por outro lado, aproximadamente um décimo (9%) conseguiram diminuir seu gasto com *capex* em mais de 20%.

Com relação ao *opex*, nesta mesma pesquisa vê-se que 70% das empresas relataram que os gastos com relação a suporte não modificaram, enquanto 28%

relataram que aumentaram mais de 20%. Já para Mike Cunningham, o programa BYOD da *Kraft Foods* ajudou a diminuir gastos com suporte (CIO, 2013c).

Além do citado acima, há os gastos com reembolso de colaboradores e transferências legais de dispositivos, que foram mencionados no capítulo anterior.

Pelo que se percebe, a proporção de empresas que conseguem economia de custos, seja em seu *capex* ou seu *opex*, é a minoria. Se o programa BYOD promove ganho de produtividade, como é a crença e a experiência de tantos executivos renomados na área, e, se por outro lado, na maioria das empresas não há diminuição alguma de custos ou até mesmo há um aumento deles, então é necessário encontrar uma explicação para isso.

Uma delas, segundo a pesquisa da CCMI, pode residir no fato de que há tantas tecnologias disponíveis para o consumidor, que os colaboradores estão levando mais deles pro trabalho, e, assim, criando mais potencial para que a organização arque com as despesas.

A CCMI cita recente pesquisa da empresa *Cisco*, desenvolvedora de tecnologias para redes de computadores, a qual diz que o número médio de dispositivos carregado por cada colaborador, nos EUA, é de 2,8 dispositivo/colaborador. A *Cisco* também prevê que, até 2014, este número passe para 3,3 dispositivo/colaborador.

Outra explicação que também reside na realidade norte-americana, é que, no modelo BE, a maioria das organizações barganha com as companhias telefônicas descontos baseando-se numa grande quantidade de planos que a empresa contrata junto à companhia para seus dispositivos móveis. Com a implementação do programa BYOD e do modelo híbrido, ela perdeu esse poder de barganha, com uma quantidade menor de planos e, por conseguinte, do desconto, aumentando a quantidade de despesas da empresa.

Todavia, definir com exatidão em que ponto as empresas estão deixando de ganhar dinheiro com o programa BYOD é extremamente difícil e, até o momento, não se conseguiu realizar isto. A conclusão é de que é preciso balancear bem os prós e contras para achar um equilíbrio para o negócio. Segundo a *Microsoft*,

quando a consumerização é planejada e gerenciada adequadamente, ela gera ganhos em produtividade e competitividade (MICROSOFT, 2013).

O que vemos com relação à lucratividade do programa, é que diversos fatores devem ser avaliados, e, mesmo assim, nem sempre é possível prever com certeza se o resultado final será de aumento dos gastos, diminuição, ou se permanecerão no mesmo patamar.

O papel da TI é analisar cuidadosamente todos estes fatores, ao fazer o planejamento do programa BYOD, e, depois de testado e implementado, estar em contínuo monitoramento, para poder fazer a alteração destes fatores, caso necessário.

Vemos que a despesa com *opex*, ou seja, suporte, em geral fica a mesma ou aumenta. Com relação ao *capex*, apesar de ser um dos objetivos principais das organizações ao implementar o programa BYOD, ele permanece como uma incógnita, sendo que as empresas muitas vezes não conseguem determinar o real motivo pelo qual ele aumenta.

Vimos que os gastos com reembolso de colaboradores e outras técnicas afins em geral não são desprezíveis. E por fim, como veremos posteriormente, o nível de risco com relação a segurança no momento ainda é moderado.

Por outro lado, há exemplos de empresas que conseguiram alcançar seu objetivo de diminuir seu *capex*, e também tiveram diminuição de gastos em outras áreas. Para a pesquisa do *Aberdeen Group*, as melhores experiências de gerenciamento do programa BYOD conseguiram reduzir as despesas com dispositivos móveis na ordem de 25% com uma controle racional e centralizado (ABERDEEN, 2013).

Portanto, percebemos que, além da análise cuidadosa de todos os fatores envolvidos, é fundamental também haver muita eficiência técnica para gerenciar a infraestrutura de TI da empresa. Além disso, é preciso alinhar a gestão dos recursos humanos da TI com essa nova realidade, baseada cada vez mais no modelo *bottom-up* de inovação tecnológica, ou, em outras palavras, consumerização.

É parte do papel da TI promover uma mudança no espaço de trabalho e na relação com o colaborador. O gestor de TI deve compreender que a realidade está mudando, e que os colaboradores também estão. Saber entender e como lidar com esse recurso humano também é fundamental para levar a organização que adere à consumerização no caminho da lucratividade.

3.3. Suporte

Para fins deste capítulo será definido como interoperabilidade a comunicação entre plataformas diferentes, e como portabilidade a capacidade de um programa, tal como um aplicativo para dispositivos móveis, ser usado em diferentes plataformas e arquiteturas de *hardware*.

Uma das idéias principais do suporte é a de que a quantidade de dispositivos móveis e de plataformas disponíveis no mercado é grande e variada e então, na empresa, ao invés de aceitar alguns e excluir outros, é preciso desenvolver uma estratégia que possibilite a aceitação de toda esta gama heterogênea de dispositivos e plataformas.

Carlos Rabello, gerente de soluções corporativas para usuário final da *Dell* Brasil, diz que, no planejamento de seu programa BYOD, a empresa se preocupou em montar uma lista de opções em soluções de suporte para lidar com um ambiente heterogêneo de plataformas móveis.

Além disso, as empresas estão aderindo cada vez mais ao desenvolvimento de *App Stores*, ou lojas de aplicativos. Segundo este conceito, as empresas possuem seu próprio portfólio de aplicativos, o qual é uma maneira ágil e flexível para as organizações proverem aos colaboradores os tipos de escolhas com que eles estão acostumados em suas vidas pessoais.

As lojas de aplicativos estão fundamentalmente mudando a forma como os colaboradores configuram e usam seus dispositivos. Além disso, as organizações

buscam maneiras para gerenciar suas aplicações e dados mais eficientemente, e isto está sendo possibilitado com a criação de *App Stores* corporativas (GREENGARD, 2013a).

Num ambiente assim, os conceitos de interoperabilidade e portabilidade são muito importantes. São duas características desejadas, embora muitas vezes dependam de fatores externos à empresa.

A interoperabilidade dos sistemas da empresa com as diversas plataformas deve ser garantida.

Existem dispositivos que possuem pouca interoperabilidade, mas são fáceis de suportar, tais com o *Blackberry,* já outros possuem muita interoperabilidade, mas são de difícil suporte. Isto deve ser levado em conta no planejamento do suporte (CIO, 2013c).

A portabilidade pode ser alcançada utilizando, no desenvolvimento de sistemas, aplicativos e *softwares* da organização, linguagens que facilitem esta portabilidade para a extensa gama de dispositivos e plataformas disponíveis no mercado.

Algumas linguagens facilitam esta implementação, tais como *Html* ou *Java*, tornando mais fácil o suporte pela TI, porém, nem sempre é viável basear aplicativos e outros *softwares* nessas linguagens.

Segundo a revista *Computerworld* Brasil, o nível de suporte oferecido para BYOD ainda é baixo. Oferecer suporte para um programa BYOD é um grande desafio para o empresariado. Como vimos, são poucos os exemplos de empresas que conseguiram abaixar seu *opex* com dispositivos móveis, muito embora, para a maioria, o nível de gastos não tenha mudado de patamar (COMPUTERWORLD, 2013b; CCMI, 2013).

Portanto, suporte é algo que ainda traz muitas incertezas. Segundo Moschella (2013) e May (2013), além da crença na produtividade, há uma crença de que os colaboradores, consumidores de tecnologia, estão se tornando mais experientes com seus próprios dispositivos. Há uma pressão maior pela personalização do

ambiente de trabalho, em contraste com a padronização, focada no modelo *top-down*, ou BE.

Muitas das novas gerações de colaboradores cresceram usando estas tecnologias, e um número muito grande conhece estas ferramentas às vezes muito melhor que a TI da empresa. A pesquisa da Avanade (2013) mostrou que, embora os serviços e aplicações mais utilizados pelos colaboradores no trabalho ainda sejam o *e-mail* e as redes sociais, os colaboradores mantêm uma expressiva utilização dos serviços e aplicações corporativos, indicando que eles têm aprendido a usar os dispositivos móveis eficientemente como ferramenta de trabalho.

Esta idéia reforçou a crença de que os gastos com suporte iriam diminuir. Porém a pesquisa da CCMI mostrou que 28% das empresas que implementaram o programa BYOD relataram que os gastos aumentaram em mais de 20%.

Os exemplos em que o *opex* diminuiu ainda são raros. Uma explicação para isso pode ser que, embora os colaboradores de fato estejam se tornando mais experientes e auto-suportáveis com seus dispositivos móveis, ainda esteja faltando uma mudança nos próprios modelos de gestão do programa BYOD por parte da TI. Moschella afirma que:

> "Para tirar vantagem da consumerização, as companhias precisam compreender e aceitar a fusão entre nossa vida pessoal e profissional. Isto significa adotar modelos diferenciados de gestão dos colaboradores e suporte" (MOSCHELLA, 2013).

Para Ted Schadler, analista da empresa *Forrester*, que realiza pesquisas de mercado a respeito da utilização de tecnologia, para gerenciar o programa BYOD é necessário mudar a forma como a TI se relaciona com o colaborador e "parar de tratar a questão como se fosse um problema de policiamento, e abordá-la como gestão de risco" (CIO, 2013d).

Como já foi mencionado, a Avanade diz que a TI deve mover da posição de rígidos controladores do uso de dispositivos móveis na empresa, para promovedores destes dispositivos, aplicativos e serviços. Deve-se focar, além das questões técnicas, nas questões humanas, de forma a compreender o fenômeno da consumerização e utilizar isto a seu favor.

A pesquisa da CCMI observa, de forma interessante, que os colaboradores teoricamente não deveriam esperar suporte técnico da TI, porém, os executivos relatam que estão fazendo o melhor que podem num ambiente de múltiplas plataformas.

Segundo a CIO Brasil (2013d), um estudo da *Unisys*, conduzido pela IDC, mostra que 61% dos executivos brasileiros de TI relatam que os colaboradores de suas empresas buscam assistência nas próprias áreas de TI das organizações quando têm um problema técnico nos aparelhos pessoais usados no trabalho.

A pesquisa da Avanade afirma que, apesar da visão de que as organizações estão lutando para alinhar seus recursos com os novos desafios e demandas criadas pela consumerização, de fato elas possuem a maior parte dos recursos que elas necessitam.

Para 91% dos executivos e 75% dos profissionais de TI, o setor de TI possui os recursos humanos e tecnológicos necessários para gerência o uso dos dispositivos móveis. Acrescenta-se que, na opinião de 84% dos executivos e 62% dos profissionais de TI entrevistados, é relativamente simples integrar os dispositivos móveis dos colaboradores, aplicativos e serviços com os sistemas da empresa.

Além disso, não obstante o orçamento das empresas já reservar consideráveis recursos financeiros para gerenciar o programa BYOD, 79% dos executivos relatam que planejam fazer novos investimentos para suportar o uso de tecnologias pessoais no trabalho.

Segundo a pesquisa da CCMI, as plataformas para dispositivos móveis estão ganhando funcionalidades em segurança com sofisticação cada vez mais ao nível da segurança exigida pelas grandes organizações, como resultado de uma interação

maior entre os fabricantes de tecnologia de consumo em massa e os desenvolvedores de soluções.

O motivo pelo qual, segundo a CCMI, os aparelhos *Blackberry* são os mais suportados pelas organizações, é devido a estes dispositivos terem sido projetados pela empresa RIM – *Research in Motion* – para ser utilizado em ambiente corporativo, tendo funcionalidades que auxiliam no suporte e segurança, devido à longa experiência da empresa fabricante neste segmento.

Um exemplo disto é relativo ao acesso remoto, tão comum em plataformas computacionais mais tradicionais no mercado, e que só agora está ficando mais facilitado para dispositivos móveis, surgindo várias soluções de desenvolvimento deste tipo de aplicação. Cada vez mais dispositivos e plataformas estão sendo projetados com a finalidade de tornar seu suporte cada vez mais ágil.

Há também um grande desenvolvimento de *softwares* que integram e centralizam várias funções de gerenciamento. São *softwares* complexos capazes de gerenciar empresas de grandes proporções e com infraestrutura de TI complexa. Um grande número de empresas de soluções em tecnologia estão desenvolvendo estes produtos com vistas ao mercado corporativo.

Portanto, como bem observou Moschella (2013), o próprio mercado esta se encarregando de oferecer soluções para auxiliar as empresas com relação a suporte e segurança. Os fabricantes de tecnologia estão projetando seus produtos para ajudar a TI a administrá-los, e preocupações estão sendo atendidas, na busca para atenuar os problemas de suporte da TI. Cabe, portanto, à empresa saber buscar e utilizar essas ferramentas.

3.4. Segurança

Como diz Moschella (2013), a consumerização tem todas as características de ser um caso clássico de tecnologia disruptiva, e isto significa que muitas organizações encontrarão dificuldades para gerenciá-la.

De acordo com estudo da *Unisys*, conduzido pela IDC, o uso de dispositivos móveis e outras tecnologias da consumerização causa sérios impactos para as organizações com relação ao suporte aos equipamentos e à segurança das informações (COMPUTERWORLD, 2013b).

Como já mencionado, Paulo Vendramini, diretor comercial da *Symantec* Brasil, diz para a CIO Brasil que: “Até então, as organizações estavam acostumadas a proteger informações associadas à infraestrutura. Com o surgimento de *cloud* e mobilidade, há perda de controle do hardware”. E logo após, continua: “O grande drama é: como continuar resguardando a informação independentemente do controle da infraestrutura?” (COMPUTERWORLD, 2013d).

A pequisa da Avanade (2013) diz que, devido à rápida expansão das tecnologias disponíveis no mercado consumidor e de sua força inovadora, as especificações de segurança das empresas não acompanharam o mesmo ritmo.

Uma prova disto é que 55% das empresas já experimentou algum tipo de incidente de segurança devido à vulnerabilidades causadas pela invasão de dispositivos móveis no ambiente de trabalho. Para 81% dos profissionais de TI, a infraestrutura da empresa precisa de melhorias para atingir o nível de segurança adequado.

Considere, todavia, que há uma barreira de proteção que independe da empresa, e a qual pode desaparecer repentinamente. Os códigos maliciosos de uma plataforma móvel não funcionam em outra plataforma. Uma importante barreira para uma ação maior destes códigos maliciosos entre os dispositivos móveis é o grande número e diversidade de plataformas móveis.

Porém, não há garantia de que o nível de proteção permaneça elevado por causa disso. Neste ponto tem seu efeito a estratégia de aceitação de uma gama heterogênea de dispositivos e plataformas, ao invés de focar em somente uma ou poucas (LAYTON, 2013).

A pesquisa da empresa Proofpoint (2013) mostra que, apesar da vasta gama de aplicativos, serviços e funções disponíveis nos dispositivos móveis, o *e-mail* continua sendo a forma de comunicação mais utilizada, com 67% da preferência de uso. Como conclusão, a empresa diz que a segurança para serviços de *e-mail* deve estar entre as prioridades máximas de um programa BYOD.

Felizmente, diz a empresa, a maioria das empresas possui tecnologias de segurança para serviços de *e-mail* tais como arquivamento de *e-mail*, segurança de *e-mail*, DLP – *Data Loss Prevention* –, e aquelas empresas que podem estender essa segurança para os dispositivos móveis estão em melhor posição de trazer o seu programa BYOD para dentro dos limites de segurança e conformidade.

Por outro lado, embora haja sérios problemas relativos a questões de segurança e que, a curto prazo, esses problemas possam ser só parcialmente solucionados, este fato não deve ser uma barreira para a implementação do programa BYOD na empresa.

O mercado irá pressionar para que as tecnologias disponíveis para o consumidor cheguem ao mesmo nível de segurança dos sistemas gerenciados pelas grandes organizações e até mesmo o exceda. Segundo ele, em algumas áreas isso já ocorreu (CIO, 2013c; MOSCHELLA, 2013).

A primeira preocupação das empresas devem ser em planejar a forma como irão realizar a transição entre o modelo *top-down*, ou BE, para o modelo *bottom-up*, ou BYOD, preferencialmente utilizando um período de teste do programa, e então monitorar, avaliar e julgar a maturidade do serviço.

Além disso, a *Computerworld* Brasil (2013d) cita que, segundo a *Symantec*, diante da explosão de dispositivos móveis, as organizações deverão adotar uma abordagem mais pró-ativa para proteger os dados corporativos, e isto significa, em muitos casos, saber antever possíveis ameaças à organização.

Como já foi dito anteriormente, para a *Proofpoint* (2013), a solução de segurança para o programa BYOD reside numa gestão moderna no colaborador, na implementação de uma política de segurança da informação que abranja também dispositivos móveis e no uso de tecnologias para gerenciamento de dispositivos móveis. Para esta empresa, as organizações que implementam segurança nestes três níveis conjuntamente, estão aptas para fortalecer a defesa dos dispositivos móveis utilizados por seus colaboradores.

Com esta visão também concorda Sêmola (2003), que chama atenção para o aspecto integrado da segurança da informação. A gestão da segurança da informação envolve pensar-se não somente nos aspectos tecnológicos, mas também nos aspectos humanos e basear-se numa política. Somente uma ação integrada nestes três níveis é que pode efetivamente assegurar a segurança da informação.

A pesquisa da Avanade (2013) diz que, como qualquer outra tendência no campo da tecnologia, a gestão da consumerização da TI requer uma combinação de cuidados com os recursos humanos, estabelecimento de normas e processos, e utilização de tecnologias para se garantir uma segurança efetiva no ambiente de negócios e se conseguir gerenciar o cronograma de mudanças que estão acontecendo na empresa.

Baseando-nos em Sêmola (2003), Moschella (2013) e May (2013), sugerimos que o diferencial da gestão da segurança da informação é o gerenciamento do recurso humano. Como já foi mencionado, os colaboradores estão utilizando os dispositivos móveis para acessar informações de trabalho independentemente da permissão da empresa.

Ou seja, de nada adianta um pesado investimento de recursos na implementação do programa BYOD e no desenvolvimento ou aquisição de soluções tecnológicas para segurança, se, com relação à gestão dos aspectos humanos, a empresa perde o controle de sua comunicação interna.

Por outro lado, como foi visto, há tantas ferramentas de segurança disponíveis, que isso auxilia as organizações a disponibilizar serviços para o

programa BYOD com um risco, que embora ainda seja moderado, se torna cada vez menor.

Estas ferramentas se baseiam em técnicas tradicionais usadas para gerenciamento de redes, tais como utilização de VPN's, *firewalls*, criptografia, autenticação, entre outras, porém, elas exigirão adaptações da TI para enfrentarem os novos problemas de gerenciamento criados pela implementação do programa BYOD.

4. BYOD NA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Após analisar os fundamentos estratégicos, este capítulo tentará mostrar alguns aspectos táticos do BYOD, e como ele pode ser inserido na política de segurança da informação da empresa.

O BYOD é definido como um programa pois deve ser planejado, desenvolvido, testado e revisado até chegar ao seu produto final: o programa implementado.

Após o programa ser implementado, ele deve ser alvo de uma revisão periódica, a fim de determinar se o seu escopo deve sofrer alteração, incluindo outras tecnologias ou não. Isto ocorre, porque o fenômeno da consumerização é dinâmico e as organizações não devem considerar que seu programa BYOD é definitivo.

Como já citado, a advogada especialista em Direito Digital, Patrícia Pinheiro, diz que um dos primeiros pontos durante o planejamento do programa BYOD é deixar muito bem definido de quem é a propriedade dos dispositivos, além de quais requisitos de segurança que o colaborador deverá seguir e quais as obrigações e limites de uso dos aparelhos (CIO, 2013a).

Um mecanismo comum é a exigência de que os colaboradores concordem expressamente com as regras do programa BYOD, ou, em outras palavras, com a política de segurança da informação para dispositivos móveis da empresa. Eles assinam documentos em que tomam ciência das normas do programa BYOD e esta tática tem sido largamente utilizada.

É preciso reconhecer que muitas vezes a TI não tem conhecimento total de que aparelhos acessam as informações da empresa. Segundo pesquisa de 2010 da *Unisys*, conduzida pela IDC, frente ao empresariado brasileiro, as empresas do Brasil não sabem quais tecnologias os colaboradores usam durante o expediente. Para se preparar para proteger as informações da empresa, é preciso fazer um

levantamento de todos os ativos relacionados a *hardware* e *software* da empresa (COMPUTERWORLD, 2013d).

Ao mesmo tempo, como diz José Antunes, gerente de engenharia de sistemas da *McAfee* Brasil:

> "Ao olhar para a segurança como um todo, a principal preocupação é em relação à perda de informações confidenciais. Mas o grande gargalo é classificar essa massa de dados: quem tem acesso, quem realmente precisa tê-lo e para onde vai" (COMPUTERWORLD, 2013d).

Portanto, após o levantamento de todos os ativos relacionados a *hardware* e *software* é preciso fazer o mesmo com relação à informação da empresa. Porém, não basta apenas fazer este levantamento, mas também classificar a informação de acordo com sua criticidade e levando-se em consideração a natureza da organização.

Após o levantamento de *hardware* e *software*, e de se levantar e classificar a informação da empresa, é preciso fazer um levantamento e uma classificação de seus colaboradores. Após estas etapas será possível definir que tipo de colaboradores, usando quais tipos de dispositivos, tem acesso a quais tipos de informações, aplicações e serviços dentro da empresa.

Por exemplo, os *tablet's* são famosos por seu excelente desempenho com relação a vídeo conferência, aplicativos que utilizam *streamming* de vídeo e outros recursos multimídia, se configurando a princípio como excelentes dispositivos para colaboradores que necessitem fazer viagens a trabalho. Porém, analisando mais de perto, vê-se que as excelentes qualidades do dispositivo podem, por exemplo, levar ao abuso do colaborador, fazendo mal uso do aparelho.

Uma vez que as empresas tenham um quadro claro da situação da empresa, elas devem começar a construir suas aplicações principais e os serviços necessários para aumentar o desempenho dos colaboradores. As aplicações e serviços

empresariais não estão otimizados para os dispositivos móveis, fazendo com que os colaboradores utilizem meios alternativos para acessá-los.

É preciso fazer com que estejam alinhados com os dispositivos móveis e suas plataformas, para a organização aproveitar melhor o potencial do programa BYOD. A criação de *app stores* corporativas é útil para isso, criado um espaço de flexibilidade dentro da empresa.

Com relação a que tipo de dispositivos serão suportados pela organização, a já citada pesquisa da revista CIO dos EUA diz que, entre as 131 empresas que permitem BYOD, a maioria apenas sugere os equipamentos que os funcionários devem usar, deixando a decisão final para cada um deles. Apenas 22% exigem que os empregados escolham os dispositivos de uma lista específica. Outros 38% permitem que os funcionários escolham qualquer dispositivo.

Segundo a opinião de alguns especialistas, a opção mais desejável é que seja feito uma lista, com os aparelhos e plataformas suportados pelo programa BYOD adotado pela empresa. Para participar do programa, o colaborador deverá ter um dispositivo móvel que conste na lista elaborada pela TI da empresa. Aqueles dispositivos e plataformas fora da lista não devem acessar as informações da empresa (CIO, 2013c).

A separação dos ambientes pessoais e corporativos é fundamental não apenas para resolver questões de propriedade, mas também para suporte e para a segurança também. A separação entre os dois ambientes pode ser implementada usado uma tecnologia específica para gerenciamento de dispositivos móveis que se baseie largamente em operações feitas através de autenticação, e com uso de criptografia na transmissão de informações.

Além desta camada de proteção, técnicas de VPN ou, mais sofisticadamente, de virtualização, que separem os dois ambientes por completo estão sendo muito difundidas, e são recomendadas por todos os autores que compõem este trabalho. O redirecionamento de projeto dos fabricantes de dispositivos móveis, como o já citado caso do *Dual Persona*, da *Telefônica*, prometem auxiliar na tarefa de separação dos ambientes.

Por outro lado, a empresa precisa monitorar os dispositivos móveis pessoais dos colaboradores que utilizam seus recursos de TI. Como já foi citado, ela deve deixar claro que tem o direito de rodar um aplicativo de segurança, analisar trilhas de auditoria ou deletar arquivos com informação corporativa quando necessário.

Mesmo com a utilização de *software* de gerenciamento automatizado, erros podem ser cometidos, como por exemplo, a exclusão de arquivos pessoais do colaborador, causando constrangimento. A empresa precisa utilizar do mecanismo de fazer com que o colaborador concorde por escrito com o monitoramento de seu dispositivo pela empresa, a fim de proteger a organização de possíveis pedidos de indenização,

Outro ponto é que todos os dispositivos devem ter aplicativos de segurança, sendo os mais básicos entre eles um aplicativo de anti-vírus e um aplicativo de *firewall* instalado no aparelho. Estes aplicativos deverão ser escolhido pela organização. A organização se reservará no direito de rodar esses aplicativos quando julgar necessário utilizando tecnologias específicas de gerenciamento de dispositivos móveis.

Com relação ao *backup*, todas as técnicas têm direcionado para que seu uso seja feito pelo próprio colaborador, sem que com isso, todavia, signifique que a empresa não possa fazê-lo se caso achar necessário. Isto porque as informações que estão contidas no dispositivo móvel do colaborador podem ser altamente concernentes aos negócios da empresa.

Nesta tarefa, serviços oferecidos, como os da nuvem, podem ser muito úteis. Há serviços que oferecem o serviço de *backup* na nuvem. E, como foi dito anteriormente, são serviços públicos que, muitas vezes, oferecem um nível de segurança maior que o nível de segurança da empresa. Este também é um exemplo de como os desenvolvedores de tecnologia deverão projetar cada vez mais produtos destinados a BYOD.

Outro aspecto importante é com relação ao furto, roubo ou extravio do dispositivo móvel. É preciso utilizar tecnologias de gerenciamento que consigam

bloquear o acesso à informação relativa à organização, ou mesmo que estes dados sejam destruídos. Já existem disponíveis no mercado mecanismos para isso.

De suprema importância para qualquer política de segurança da informação, e não é diferente no caso do programa BYOD, é com relação á conscientização e treinamento dos colaboradores. Neste ponto, parece haver um longo caminho a percorrer. Segundo a pesquisa da Avanade (2013), somente 38% das empresas está investindo em treinamento para os colaboradores em geral, e uma proporção ainda menor, 35%, pretende investir em treinamento para o pessoal especializado em TI.

A conscientização e treinamento dos colaboradores será fundamental para o sucesso dos programas BYOD. Relacionado a isso, está fato de o programa BYOD dever ser cumprido em etapas, sendo introduzido na organização aos poucos, e somente após a realização de testes de implementação. E, mesmo após a implementação do programa, como diz Mike Cunningham, diretor de tecnologia da *Kraft Foods*, é necessário realizar testes metódicos para saber o que precisa ser controlado e que pode ser liberado (CIO, 2013c).

Como se trata de uma questão de gerenciamento de riscos, é importante haver o planejamento dos riscos e a criação de planos de emergência, de contingência e de continuidade de negócios relativo ao programa BYOD e ao uso de dispositivos móveis que acessam informação da empresa. Pelo fato da tendência ser das organizações se basearem cada vez mais nesse uso, a falta de tais planos pode ser desastrosa para os negócios das empresas. As empresas que possuem estes planos também melhoram sua imagem comercial no mercado.

Por fim, é importante que todo o material relativo a documentação de colaboradores, quando se tratar do programa BYOD, deve ser arquivado organizadamente pela TI. Quando houver problemas jurídicos com colaboradores, é a TI que deve transmitir as informações para o departamento jurídico ou de recursos humanos e não o contrário.

As outras documentações relativas a ativos ou mesmo as informações digitais, tais como trilhas de auditoria, devem permanecer com a TI, e não

espalhadas com a empresa. Na eventualidade de a organização ser alvo de fiscalização ou auditorias, a TI deverá estar organizada para comprovar sua conformidade.

A seguir serão apresentados dois estudos de caso, ambos do setor de educação. O primeiro, do Colégio Mackenzie, apresentará uma solução de programa BYOD baseada no uso de tecnologia central de gerenciamento. Já o segundo, do SENAC – Serviço Nacional de Aprendizagem Comercial –, se trata de uma política de segurança, e será apresentado por mostrar uma solução que não conta com *software* especializado em gerenciamento e, portanto, precisa basear-se na criação de normas e na gestão de pessoas.

4.1. Estudo de Caso: Instituto Mackenzie de São Paulo

O Mackenzie é uma instituição educacional que oferece todos os níveis de formação, da educação básica à pós-graduação, e, atualmente, tem sua rede presente em São Paulo, Brasília, Campinas e Rio de Janeiro.

No Instituto Mackenzie de São Paulo, a alta diretoria aderiu ao uso de dispositivos móveis. Constantemente, pessoal da diretoria e da alta administração viaja tanto no Brasil como para o exterior e necessitam consultar calendários da organização, ver *e-mails* etc., acessando informações corporativas com seus dispositivos.

Tablet's foram distribuídos pela TI a todos os membros do conselho com o objetivo de tornar mais ágeis as freqüentes reuniões, e para facilitar o trabalho dos colaboradores durante viagens.

O problema está em oferecer à diretoria uma maneira segura de acessar estas informações utilizando uma tecnologia central de gerenciamento. Para isso o Mackenzie adquiriu o *software* EMM – *Enterprise Mobility Management* – da

empresa *AirWatch*, líder mundial em desenvolvimento de tecnologia para gerenciamento de dispositivos móveis.

A solução da *AirWatch* permite o acesso automático a conteúdo digital da organização, como documentos eletrônicos e *e-mail,* assim como provê acesso à Internet atendendo às necessidades de segurança e gerenciamento dos dispositivos e aplicativos.

O EMM utiliza três técnicas integradas para este gerenciamento. O MCM – Gerenciamento de Conteúdo Móvel – permite a distribuição e o acesso seguro a documentos através de um aplicativo instalado no dispositivo móvel.

O SCL – *Secure Content Locker* – permite à diretoria acessar os recursos corporativos de qualquer lugar com seus dispositivos móveis e gerenciamento, além de oferecer um cômodo gerenciamento das reuniões para os executivos.

O MAM – *Gerenciamento de Aplicativos Móveis* – é fundamental para a transmissão de aplicativos internos, como, por exemplo, o canal de TV da escola, de forma que os executivos têm sempre acesso às noticias da instituição. O MAM faz o *upload* no SCL de importantes segmentos de *web clips* e os envia aos membros da diretoria, que não têm tempo de assistir a um programa inteiro.

O Mackenzie teve um caso de furto e pôde apagar todas as informações do dispositivo. O gerenciamento através do EMM da *AirWatch* permitiu apagar os dados deste dispositivo furtado rapidamente e restaurar imediatamente e de forma simples toda a configuração, conteúdos e aplicativos em um novo dispositivo (AIRWATCH, 2013).

Pode-se observar que a estratégia da instituição, atualmente, se concentra em uma solução baseada somente na aquisição de tecnologia de empresa desenvolvedora terceirizada, que implantou uma solução a curto prazo. Porém, o instituto planeja dar continuidade ao projeto de mobilidade em uma maior escala, talvez indicando que, se quiser expandir este programa na organização, precisará definir estrategicamente outros aspectos além do tecnológico.

4.2. Estudo de Caso: SENAC de São Paulo

Para o segundo estudo de caso escolhemos a situação do SENAC de São Paulo, o qual, em 2011, criou uma política de segurança da informação que deve ser seguida por todos os funcionários das 54 unidades espalhadas pelo estado e a qual possui um capítulo específico sobre dispositivos móveis.

Por se tratar de uma política de segurança da informação relativo ao uso destes dispositivos para fins de trabalho, ou seja, de um programa BYOD, ele deve ser possível de ser organizado estrategicamente nos aspectos relativos á propriedade, à produtividade/motivação, ao suporte e à segurança. Os itens relativos ao capítulo sobre dispositivos móveis na política de segurança da informação podem ser organizados da seguinte forma:

1) Propriedade:

- Define o modelo BYOD a seguir como híbrido ao definir que os dispositivos são propriedades da instituição ou, quando do colaborador, devem ser aprovados e permitidos pela Gerência de Sistemas;
- Deixa o colaborador ciente de que é o responsável por todo *software* que não tenha sido instalado ou autorizado pela Gerência de Sistemas;
- Deixa o colaborador ciente de que será considerado uso indevido e infração dos direitos autorais o uso não autorizado de softwares instalados nos dispositivos móveis pertencentes à empresa;
- Deixa o colaborador ciente de que assumirá todos os riscos pelo uso indevido do dispositivo, sendo o responsável por danos diretos ou indiretos, presentes ou futuros, que venha a causar à instituição ou a terceiros;
- No capítulo “Das Responsabilidades Específicas”, item 5 – Do Monitoramento e da Auditoria de Sistemas, a empresa deixa o colaborador ciente de que poderá monitorar os dispositivos da organização, e que as trilhas de auditoria

geradas poderão ser analisadas caso seja necessário identificar acessos de colaboradores.

2) Produtividade/Motivação:

- Foca na motivação quando diz que permite a utilização de dispositivos móveis para “facilitar a mobilidade”, e foca a produtividade quando diz que quer facilitar o fluxo de informação entre os colaboradores;
- Foca produtividade e motivação quando permite o uso dos dispositivos utilizando banda larga de locais conhecidos pelo colaborador tais como sua casa, hotéis, fornecedores, clientes etc.

3) Suporte:

- O suporte técnico dos dispositivos móveis de propriedade do SENAC São Paulo deverá seguir o mesmo fluxo de suporte contratado pela instituição;
- Todo dispositivo móvel pessoal utilizado na infraestrutura de TI deve submetido à autorização pela Gerência de Sistemas;
- Todo dispositivo móvel pessoal que não for submetido à autorização não será validado para uso e conexão da rede corporativa.

4) Segurança:

- Faz uma classificação de seus colaboradores ao estender a validade do capítulo sobre dispositivos móveis da política de segurança somente a aqueles que utilizam tais dispositivos na empresa;
- Deixa o colaborador ciente de que pode inspecionar o dispositivo a qualquer momento, para encontrar vulnerabilidades de segurança;
- Deixa o colaborador ciente sobre o compromisso de sigilo para com a organização;

- Deixa o colaborador ciente de que é sua responsabilidade fazer *backups* periódicos;
- Define que os acessos dos colaboradores serão autenticados por senha;
- Deixa o colaborador ciente de que não pode alterar as configurações lógicas sem a autorização e presença de um membro da Gerência de Sistemas;
- Deixa o colaborador ciente de como proceder em caso de furto ou roubo do dispositivo.

O caso do SENAC difere do Instituto Mackenzie pois, com relação aos dispositivos móveis particulares, ele somente autoriza que se conecte à rede da instituição, não permitindo acesso a informação restrita ou confidencial. Já para o Instituto Mackenzie há, de fato, um programa BYOD completo, no sentido de que os dispositivos móveis particulares acessam informações, aplicações e serviços da organização, integrados e centralizados em uma tecnologia de gerenciamento.

Não obstante, foi efetivamente possível organizar estrategicamente os 17 pontos do capítulo sobre dispositivos móveis da política de segurança em termos de propriedade, produtividade/motivação, suporte e segurança. O SENAC demonstra um exemplo de como implementar um programa BYOD, mesmo não completo, utilizando-se pouco recurso tecnológico.

É interessante notar que, quando há carência do recurso tecnológico, o recurso de utilização de normas escritas e a gestão dos colaboradores assume papel principal. Dos 17 pontos, 8 iniciam com “deixa o colaborador ciente de que”, significando que se baseia na ciência do colaborador. Na falta de uma tecnologia de gerenciamento que faça isso automaticamente, é necessário utilizar o mecanismo de buscar o aceite por escrito (SENAC, 2013).

5. CONSIDERAÇÕES FINAIS

O fenômeno da consumerização é mundial. Nos países centrais como os EUA, Europa, Japão, tigres asiáticos e China, a consumerização já tem uma expansão predominante, enquanto nos países periféricos, como no caso do Brasil, ainda está em suas primeiras expressões.

A consumerização é claramente uma tecnologia disruptiva, com o que concordam outros autores, e pode ser classificada como uma inovação tecnológica com algumas conseqüências sociais. Nos países centrais a sua fase onde é vista como “ameaça” já está bastante amadurecida, e parece pronta para começar a entrar na segunda fase onde será vista como “comum” (ACKERMAN; GUZZO; GILBERT, 2013).

No caso do Brasil, a consumerização como tecnologia disruptiva está claramente na primeira fase, quando é vista como “inofensiva”, não parecendo, no momento, estar pronto para entrar na segunda fase da evolução de tecnologias disruptivas, conforme a teoria de Christensen citada por Moschella (2013).

Como conseqüências sociais da consumerização, além do intenso ritmo de inovação tecnológica produzida pelas indústrias voltadas para o mercado de consumo em massa, pode-se observar o crescimento da importância do valor comercial do programa BYOD, a mudança do conceito de trabalho e espaço de trabalho e a maior integração entre os ambientes pessoal e profissional.

É preciso avaliar esta dimensão social da consumerização para melhor analisar estrategicamente o programa BYOD nas empresas. Além disso, é papel da TI das organizações compreender esta mudança na sociedade, e não focar somente no aspecto tecnológico, mas também humano.

Para efetivamente garantir a segurança da informação nas empresas, a TI precisa desenvolver uma solução baseada na criação de uma política de segurança, na implantação de tecnologia (própria ou terceirizada) para centralizar o

gerenciamento dos dispositivos móveis e na gestão moderna e flexível dos recursos humanos.

Estrategicamente, foi observado que é possível analisar a questão do programa BYOD em termos de propriedade, produtividade/motivação dos colaboradores, suporte e segurança. Durante o estudo de caso do SENAC São Paulo, foi visto que todos os seus itens se relacionam com ao menos um destes quatro aspectos estratégicos.

Por serem aspectos estratégicos, não há um limite rígido entre eles, por exemplo, questões de suporte se relacionam com de segurança, e vice-versa, porém, dentro de um contexto, um dado problema pode ser analisado em termos de propriedade, produtividade/motivação dos colaboradores, suporte e segurança, mostrando o aspecto integrado desta estratégia.

Observou-se que, não obstante a forte crença do empresariado a respeito do aumento da produtividade e da motivação dos colaboradores, não há, até o momento, nenhum dado ou pesquisa que comprove definitivamente que, de fato, isto ocorre.

Vimos também que a diminuição de despesas com dispositivos móveis é um dos objetivos principais do programa BYOD, e os aspectos de propriedade, suporte e segurança, no momento atual, têm mais onerado que agregado às organizações. Poucos são os exemplos que conseguiram diminuição de despesas com o programa BYOD.

Porém, foi visto que, quanto maior a racionalização e organização do programa, maior as chances de se alcançar este objetivo. A racionalização deve vir acompanhada da implementação de uma sólida política de segurança, de grande apuro técnico e da gestão moderna dos colaboradores para que se desenvolva uma solução que consiga diminuir os custos do programa.

A conclusão final deste trabalho é que BYOD é viável e oferece ganhos intangíveis, tais como fortalecimento da imagem no mercado, produtividade e motivação dos colaboradores, e tangíveis, tais como diminuição de gastos com aquisição e substituição de dispositivos móveis e suporte, porém, que estes

benefícios não são algo garantido por simples adoção e implementação de uma política de segurança.

A gestão deve ser estratégica, baseada numa ação conjunta de criação de política de segurança, implementação de tecnologia de gerenciamento central e gestão moderna de recursos humanos, e, fundamentalmente importante, a transição entre o modelo tradicional e BYOD deve ser extremamente bem planejada. Desta forma, e com a revisão e readequação periódica do programa, é possível se chegar, a médio-prazo, em uma fórmula que leve a empresa à melhoria de sua relação custo-benefício com a consumerização.

6. REFERÊNCIAS BIBLIOGRÁFICAS

ABERDEEN Group. *Wireless Expense Management: Control International Roaming and the BYOD Revolution*. Disponível em: <http://www.aberdeen.com/Aberdeen-Library/7240/RA-wireless-expense-management.aspx> Acesso em: maio 2013.

ACKERMAN, E.; GUIZZO, E. *5 Technologies That Will Shape the Web:* innovations that will make the web smarter and sleeker and irresistibly more social, too. Disponível em: <http://spectrum.ieee.org/telecom/internet/5-technologies-that-will-shape-the-web> Acesso em: maio 2013.

AIRWATCH. *Mackenzie gerencia documentos confidenciais com a solução Secure Content Locker da AirWatch*. Disponível em: <http://www.mdmsolutions.com.br/Cases/AirWatch_Case_Study_Mackenzie.pdf> Acesso em: maio 2013.

AVANADE. *Global Survey: dispelling six myths of consumerization of IT.* Disponível em: <http://www.avanade.com/Documents/Resources/consumerization-of-it-executive-summary.pdf> Acesso em: abr. 2013.

BORG, A. *BYOD: Hidden Costs, Unseen Value.* Disponível em: <http://www.computer.org/portal/web/Aberdeen-Group/content?g=6012563&type=blogpost&urlTitle=byod%3A-hidden-costs-unseen-value> Acesso em: abr. 2013.

CCMI. *Mobility temperature check: just how hot is BYOD?* Disponível em: <http://www.webtorials.com/main/resource/papers/CCMI/paper1/Just-How-Hot-Is-BYOD.pdf> Acesso em: abr. 2013.

CIO. Now Digital Business. *Aprenda a evitar riscos com a política de BYOD.* Disponível em: <http://cio.uol.com.br/gestao/2012/10/04/aprenda-a-evitar-riscos-com-a-politica-de-byod/> Acesso em: maio 2013a.

(_____). Now Digital Business. *BYOD: Por onde começar?* Disponível em: <http://cio.uol.com.br/gestao/2012/08/13/byod-por-onde-comecar/> Acesso em: abr. 2013b.

(_____). Now Digital Business. *Consumerização: 9 coisas que é preciso saber.* Disponível em: <http://cio.uol.com.br/gestao/2011/10/03/consumerizacao-9-coisas-que-e-preciso-saber/> Acesso em: abr. 2013c.

(_____). Now Digital Business. Gerenciar *o BYOD: não há certo ou errado, caro ou barato*. Disponível em: <http://cio.uol.com.br/gestao/2012/07/05/gerenciar-o-byod-nao-ha-certo-ou-errado-caro-ou-barto/> Acesso em: abr. 2013d.

COMPUTERWORLD. Now Digital Business. *BYOD obriga TI a rever políticas de segurança.* Disponível em: <http://computerworld.uol.com.br/gestao/2012/09/13/byod-obriga-ti-a-rever-politicas-de-seguranca/> Acesso em: maio 2013b.

(_____). Now Digital Business. *Consumerização cresce, mas faltam políticas para uso*. Disponível em: <http://computerworld.uol.com.br/tecnologia/2011/07/14/consumerizacao-cresce-mas-faltam-politicas-para-uso/> Acesso em: abr. 2013c.

(_____). Now Digital Business. *Indústria aprimora protagonistas do BYOD*. Disponível em: <http://computerworld.uol.com.br/tecnologia/2012/06/29/industria-aprimora-protagonistas-do-byod/> Acesso em: abr. 2013d.

(_____). Now Digital Business. *Mobilidade: mais produtividade e menos segurança?.* Disponível em: <http://computerworld.uol.com.br/seguranca/2011/06/01/mobilidade-mais-produtividade-e-menos-seguranca/> Acesso em: abr. 2013d.

(_____). Now Digital Business. *O que a consumerização realmente significada para as empresas?* Disponível em: <http://computerworld.uol.com.br/tecnologia/2011/08/12/o-que-a-consumerizacao-realmente-significa-para-as-empresas/> Acesso em: abr. 2013e.

FOLHA de São Paulo. *Smartphones representam 49% das vendas de celulares no 1º trimestre.* Disponível em: <http://www1.folha.uol.com.br/mercado/2013/04/1269257-smartphones-representam-49-das-vendas-de-celulares-no-1-trimestre.shtml> Acesso em: maio 2013.

FORBES. *US Q3 handset market: 80% smart and Apple has over half.* Disponível em: <http://www.forbes.com/sites/benedictevans/2012/11/09/us-q3-handset-market-80-smart-and-apple-has-over-half/> Acesso em: maio 2013.

GILBERT, J. B. *Confronting Disruptive Innovation*. Disponível em: <http://lexicon-systems.com/pubs/itinsight/ITInsight1212.pdf> Acesso em: maio 2013.

GREENGARD, S. *Apps Crash the Enterprise.* Disponível em: <http://cacm.acm.org/news/159173-apps-crash-the-enterprise/fulltext> Acesso em: maio 2013a.

GREENGARD, S. *How Steve Jobs Revolutionized Business.* Disponível em: <http://cacm.acm.org/opinion/articles/149292-how-steve-jobs-revolutionized-business/fulltext> Acesso em: maio 2013b.

IDC. *IT Decision Makers Feeling the Pressure to Adopt Bring-Your-Own-Device.* Disponível em: <http://www.idc.com/getdoc.jsp?containerId=prAU23377712#.UWXKIb2K5kI> Acesso em: abr. 2013.

LAYTON, J. *How Cell-phone Viruses Work.* Disponível em: <http://electronics.howstuffworks.com/cell-phone-virus.htm> Acesso em: maio 2013.

LOBO, A. P. *Brasil tem um celular por habitante.* Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=24351&sid=17#.Ua4aj71Cg_B> Acesso em: abr. 2013.

MAISTO, M. *Intel Offers an Image of the Workplace of the Future*. Disponível em: <http://www.eweek.com/mobile/intel-offers-an-image-of-the-workplace-of-the-future/> Acesso em: maio 2013.

MAY, T. *The Impact of Consumerization of IT:* turning BYOD, the cloud, and other trends to your advantage. Disponível em: <http://www.cadence9.com/wp-content/uploads/2012/10/The-Imp0061ct-of-Consumerization-of-IT.pdf> Acesso em: abr. 2013.

MICROSOFT Corporation. *Strategies for Embracing Consumerization.* Disponível em: <http://download.microsoft.com/download/E/F/5/EF5F8B95-5E27-4CDB-860F-F982E5B714B0/Strategies%20for%20Embracing%20Consumerization.pdf> Acesso em: maio 2013.

MOREIRA, E. *Número de smartphones já supera o de celulares, nos EUA*. Disponível em: <http://www.techtudo.com.br/noticias/noticia/2012/03/numero-de-smartphones-ja-supera-o-de-celulares-nos-eua.html> Acesso em: abr. 2013.

MOSCHELLA, D., et al. *The 'Consumerization' of Information Technology:* position paper. Disponível em: <http://www.smaele.nl/edocs/Taylor-Consumerization-2004.pdf> Acesso em: maio 2013.

PALÁCIO do Planalto. *Lei Nº 12.551.* Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12551.htm> Acesso em: maio 2013.

PROOFPOINT. *Proofpoint 2011 Consumerized IT Security Survey.* Disponível em: <http://www.proofpoint.com/datasheets/security-and-compliance-research/Proofpoint-Consumerization-of-IT-Security-and-Compliance-Survey-2011.pdf> Acesso em: maio 2013.

SCRIVANO, R. *Mais de 30% da população já acessam a internet por dispositivos móveis.* Disponível em: <http://oglobo.globo.com/tecnologia/mais-de-30-da-populacao-ja-acessam-internet-por-dispositivos-moveis-8066384> Acesso em: abr. 2013.

SÊMOLA, M. *Gestão da Segurança da Informação*: uma visão executiva. Rio de Janeiro: Elsevier, 2003.

SENAC. *PSI – Política de Segurança da Informação:* documento de diretrizes e normas administrativas. Disponível em: <http://www.sp.senac.br/normasadministrativas/psi_normas_administrativas.pdf> Acesso em: maio 2013.

TAURION, C. *A vez do BYOC (Bring Your Own Cloud).* Disponível em: <http://www.tiespecialistas.com.br/2012/10/a-vez-do-byoc-bring-your-own-cloud/#.UaYU1tiMH3V> Acesso em: maio 2013a.

TAURION, C. *O processo de consumerização*. Disponível em: <https://www.ibm.com/developerworks/community/blogs/ctaurion/entry/o_processo_de_consumeriza_C3_A7_C3_A3o10?lang=en> Acesso em: maio 2013b.

TELECO. *Estatísticas de Celular no Mundo*. Disponível em: <http://www.teleco.com.br/pais/celular.asp> Acesso em: abr. 2013.

TRACKVIA. *The Rise of BYOD*: infographic. Disponível em: <http://www.trackvia.com/blog/infographics/bring-your-own-devices-to-work-trend-infographic> Acesso em: abr. 2013.