BYOD E CONSUMERIZAÇÃO EMPRESARIAL

Franklin Félix Faustino*

Sérgio Piter Nogueira**

RESUMO

Este trabalho apresenta uma revisão de literatura da área de tecnologia e segurança da informação voltado para a nova era das oportunidades e tráfego da informação através dos dispositivos móveis oriundos da empresa e/ou do empregado. Objetiva-se discutir sobre tais tecnologias e suas fragilidades quanto a dados sigilosos dos quais os mecanismos e métodos existentes podem vir a ser utilizados para minimizar o impacto de acessos indevidos, perda e riscos de roubo de informações relevantes à instituição. Evidenciou-se que as empresas devem se atentar mais à identificação e implantação, utilização e controle das inovações tecnológicas dentro do setor organizacional, trazendo maior performance e qualidade ao serviço como um todo.

Palavras chave: Tecnologia. Segurança da Informação. BYOD. Consumerização.

ABSTRACT

This paper presents a literature review of technology and information security areas focused on the new era of opportunities and traffic of information through the mobile devices of the company and / or the employee. The objective is to analyze these technologies and their fragilities regarding the confidential data from existing mechanisms and methods that can be used to minimize the impact of improper access, loss and risks of theft of relevant information to the institution. It was evidenced that the organizations should be more attentive to the identification and implantation, use and control of the technological innovations within the

*Graduado em Sistema de Informação pelo Centro Universitário de Patos de Minas - UNIPAM, Especialista em Gestão em Tecnologia da Informação pela Faculdade Pitágoras e MBA em Gerenciamento de Projetos pela mesma instituição. Atua como docente nos cursos de Engenharia Elétrica, Engenharia Civil e Engenharia de Produção da Faculdade FINOM de Patos de Minas, ministrando matérias relacionadas a Tecnologia da Informação e Programação. ffelix.ti@gmail.com.

**Graduado em Sistemas de Informação pela Universidade de Uberaba, especialista MBA em Gestão Empresarial pela Universidade Federal de Uberlândia com mestrado em andamento em Ciência da Computação pela Universidade Federal de Uberlândia.

organizational sector, bringing higher performance and quality to the service as a whole.

Keywords: Technology. Information security. BYOD.

1 INTRODUÇÃO

No ambiente coorporativo acelerado, os recursos pessoais de tecnologia, como *tablets* e *smartphones*, são cada vez mais utilizados por funcionários como ferramentas para alavancar a produtividade, obter melhor eficiência e proporcionar vantagem competitiva frente aos concorrentes, devido ao acesso rápido e maior flexibilidade para os funcionários (DODT, 2012).

Diante deste crescente avanço das tecnologias voltadas para dispositivos móveis, os mesmos têm se tornado indispensáveis, principalmente no campo empresarial. No entanto, ao passo que ocorre esta evolução também surgem os questionamentos com relação à segurança destes dispositivos, principalmente se tratando do uso dos equipamentos dos funcionários em ambiente organizacional. Muitas empresas não se preocupam com esta nova abordagem tecnológica e muitas ainda nem a conhecem, fato que pode ser justificado devido à falta de informação, principalmente das vantagens, riscos e meios de segurança utilizados para saná-los.

Considerando-se sua diversidade, acredita-se que como os dispositivos móveis são tecnologias recentes, muitas empresas e funcionários ainda não possuem informações relevantes ao uso correto ou prejudicial destes meios. E em alguns casos a difícil problemática dos colaboradores seguirem as regras impostas a acessos e recursos tecnológicos se resumem ao não entendimento do porquê de todo este controle e a falta de informações referentes aos riscos empresariais. Muitas vezes as organizações, não possuem informações de como aliar a tecnologia tanto fornecida pela empresa quanto do próprio funcionário, à segurança da informação de maneiras corretas e eficazes, e não utilizam políticas de segurança eficientes e aplicações disponíveis para tal.

A fim de ampliar o conhecimento e discussão através de uma revisão de literatura sobre o tema em questão, este trabalho tem como objetivo fundamental aprofundar-se na temática: *Bring Your Own Device* (BYOD) e consumerização

dentro das empresas e organizações, quais os benefícios, os problemas e como trabalhar a segurança da informação neste enfoque.

2 AS TECNOLOGIAS DE INFORMAÇÃO NAS ORGANIZAÇÕES

Observa-se o constante desenvolvimento das tecnologias de informação (TI) como instrumentos responsáveis pela organização das novas formas de trabalho, pois elas possibilitam a sua expansão para os mais diversos locais (RODRIGUES, 2010).

Neste contexto, os dispositivos móveis ganham cada vez mais espaço e importância dentro das empresas, sendo exigência no mundo profissional, e pode-se citar que entre os diversos benefícios proporcionados está a flexibilidade que se articula com a expansão do uso da *web*, possibilitando respostas em tempo real, além da inexistência da necessidade de um espaço físico geográfico para campo de trabalho (DODT, 2012).

Devido as exigências em busca da mobilidade, tem-se notado cada vez mais o avanço da tecnologia visando possibilitar equipamentos com maior performance, velocidade e capacidade de armazenamento, como por exemplo os *notebooks*, *tablets*, discos rígidos externos, *pen-drives*, entre outros que também são classificados como dispositivos móveis (FALCÃO, 2011).

O autor ainda aponta que os meios mais utilizáveis, como *pen-drive* e *Hard Disk* externos, tornam o compartilhamento da informação ou dado dentro de um recinto muito mais prático e ágil, como por exemplo, passar fotos e documentos de um microcomputador para um *notebook.* Essa praticidade acaba com a necessidade de acesso a redes ou *internet* para que isso aconteça, sendo que em alguns casos esses últimos poderiam ser entendidos pela empresa como meios inseguros.

Os dispositivos móveis como *tablets*, *smartphones* e *notebooks*, passaram a ser uma importante ferramenta midiática, através do acesso da *internet*, a rede local da organização e todos os seus recursos passam a ser móveis, proporcionando diversos benefícios, como vendas em tempo real, possibilidade de controle de compra e venda de produtos, que permitem ao usuário acesso a informações, aplicações, recursos e serviços em qualquer hora, utilizando da infraestrutura de redes sem-fio (LEMOS, 2007).

Castells (2007) faz uma análise do que ocorreu após a inovação tecnológica através dos dispositivos móveis, por meio do exemplo do profissional de vendas, que exerceu sua função durante muito tempo associada à liberdade de horários e tempo de serviço, e, atualmente, esse profissional viaja controlado por dispositivos móveis. A lógica da métrica passou do relógio de ponto da fábrica para a tela do computador ou do telefone celular.

O uso dos dispositivos móveis no mundo do trabalho, de acordo com Rodrigues (2010), se articula com os anseios de flexibilidade, pois estes recursos evitam a rotina burocrática e proporcionam novas estruturas de poder e controle.

Segundo a IDC Brasil (2016, s.p.) o país fechou em baixa o ano de 2015 com queda de 13.4% nas vendas de *smartphones*, sendo comercializadas cerca de 47 milhões contra os 54.5 milhões referentes a 2014. Porém, ainda segundo a mesma pesquisa “Em 2015, houve uma mudança no comportamento dos consumidores, que passaram a investir em celulares mais caros.”, o que determina o posicionamento da população por preferências em melhorias tecnológicas, propiciando uma resposta mais rápida do aparelho ao uso do dia a dia.

Conforme a pesquisa de Vieira (2015), em novembro de 2015, 41% dos brasileiros navegavam *online* através de múltiplas plataformas a cada mês e,59% do tempo gasto *online* no Brasil, acontecia no meio *mobile*, e a perspectiva é que este número aumente consideravelmente ao longo dos anos.

Anderson e Raine (2008) ressaltam que há previsões de que, em 2020, os dispositivos móveis sejam o maior meio de acesso à *internet*. Este fato está relacionado principalmente com a evolução *wi-fi*, o que intensifica e valoriza o estado permanente de conexão e tem impulsionado a expansão do domínio móvel. Assim, o mundo da conexão deixa as restrições impostas pelos computadores e passa a se expandir para a palma da mão.

A cada dia surgem novas tecnologias relacionadas a inovações com dispositivos móveis, como os *iPad*, *smartphones* e *tablets*, transformando-se em uma importante ferramenta para funcionários, organizações e acadêmicos, propiciando acesso rápido e fácil em qualquer lugar e hora a qualquer tipo de informação, por meio de recursos próprios para navegação e acesso, ou ainda se conectando a redes alheias (FLEISHMAN, 2010).

Juntamente com o crescimento do uso de dispositivos móveis, cresce também a utilização dos *Web Services*, que constituem um modelo de partilha que permite publicação de rotinas e métodos acessíveis pela *Internet*, proporcionando uma interface transparente para o cliente e facilidade de integração de diferentes aplicações, incluindo os dispositivos móveis (MILLER, 2001).

Por outro lado, juntamente com a criação destes dispositivos móveis, surge também o interesse na criação de vírus e outros métodos para roubo de dados pessoais. A proximidade destes com os computadores que desempenham funções do dia adia são cada vez maiores (MILLER, 2001). Estas características fazem com que os usuários guardem nas memórias destes dispositivos um número crescente de informações sigilosas como senhas dos mais variados serviços, anotações e *e-mails* corporativos. Esta praticidade faz com que as pessoas estejam mais conectadas à *internet*, seja através de 3G ou *wi-fi*, o que aumenta consideravelmente o interesse para atividades maliciosas (FLEISHMAN, 2010).

3 BYOD ECONSUMERIZAÇÃO

Com o surgimento da computação o acesso aos sistemas era bem restrito, começando primeiro por cartões perfurados e depois por terminais, que eram equipamentos ligados e acessados somente dentro dos escritórios, mas, com a chegada do computador pessoal, os usuários passaram a utilizar os recursos tecnológicos com mais facilidade, porém o equipamento e controle de todo acesso ao conteúdo dos computadores continuava sendo responsabilidade dos profissionais de tecnologia dentro da organização (ANDERSON; RAINIE, 2008).

Com a evolução constante do setor tecnológico, os funcionários algumas vezes possuem recursos tecnológicos e equipamentos superiores aos fornecidas em seus locais de trabalho, implicando em uma descentralização do controle de tráfego de dados e acessos indevidos a informações confidenciais, pela preferência da utilização de seus dispositivos particulares (FLEISHMAN, 2010).

Devido ao crescimento rápido destas tecnologias, as empresas acabaram sendo bombardeadas com novos padrões de trabalho e arquiteturas decorrentes da invasão de novos dispositivos pessoais ao ambiente profissional, os quais são denominados BYOD e consumerização (LOBO, 2013).

Segundo Taurion (2015) pode-se definir consumerização quando o dispositivo, seja ele *tablet*, *notebook* ou *smartphone* é cedido pela empresa para uso do funcionário, mas existem discussões empresariais sérias a respeito da utilização destes pelos funcionários para outros fins que não somente ao uso profissional. Por outro lado, o BYOD é o termo que se refere ao dispositivo tecnológico do próprio funcionário, e este prefere utilizá-lo no seu ambiente de trabalho em vez de usar os oferecidos pela própria organização, o que resulta na maioria das vezes em um avanço significativo do desempenho e qualidade do serviço prestado pelo próprio funcionário.

A utilização de dispositivos pessoais no local de trabalho pode ser benéfica em alguns aspectos, possibilitando maior produtividade, flexibilidade, liberdade e escolha, traduzindo em uma melhor eficiência dos serviços prestados. Apesar desta política possuir falhas e alguns riscos, bem como a questão primordial de segurança de dados, a grande maioria das organizações que abraçam a política BYOD, encontram seus funcionários sempre mais felizes, produtivos e colaborativos em prol do sucesso como um todo (SINGH, 2012).

Conforme as características do mercado atual de TI os profissionais desejam ter a flexibilidade de utilizar o próprio dispositivo, mesmo que diversos deles acabem trabalhando mais que a carga horária diária normal (LEMOS, 2007).

Falcão (2011) enfatiza que a termologia BYOD proporciona um acesso e vínculo ao serviço contínuo mesmo fora do local de trabalho, permitindo uma maior flexibilidade e disponibilidade profissional em qualquer hora e lugar, além de permitir ao funcionário usufruir de ferramentas de sua preferência, o que alavanca maior ganho de produtividade e performance profissional.

O objetivo da utilização do BYOD, mesmo com todo aparato regulamentado de segurança que deve ser seguido, é de realmente simplificar o serviço do funcionário. Devido à implementação deste conceito os dados, informações, relatórios, gráficos, entre outros documentos importantes e necessários a todo momento referente à organização estarão prontamente disponíveis e atualizados para uso em seus próprios dispositivos pessoais, os quais, o funcionário já se encontra acostumado e familiarizado através da utilização diária e o usufruem de uma forma mais eficiente e prazerosa (GILMORE; BEARDMORE, 2013).

Outro lado positivo da implementação de BYOD nas organizações e empresas é a diminuição dos ativos empresariais e dos custos de *hardware*, contudo, tem-se maiores gastos financeiros inerentes à segurança da informação tanto internas quanto externas, relacionadas à questão de perda ou roubos de aparelhos dos funcionários que podem vir a conter informações sigilosas e estratégicas de toda a organização (SINGH, 2012).

Um problema associado à consumerização e BYOD refere-se ao fato de ainda não haver uma solução *open source*, gratuita ou de baixo custo, além do fato dos grandes fornecedores de soluções estarem atentos somente para o mercado de grande porte, oferecendo soluções onerosas, e que demandam *hardware* robusto para serem implantadas (TAURION, 2015).

Segundo a Computer Word (2015) um estudo feito com empresas norte-americanas indicou que muitas estão se afastando da termologia BYOD. A pesquisa ressalta que 53% das companhias entrevistadas proíbem que funcionários tragam seus dispositivos móveis e preferem fornecer *smartphones* e *tablets* corporativos para os seus trabalhadores, e apenas 7% dos entrevistados disseram que permitem uma política completa BYOD onde a empresa não se responsabiliza por dispositivos. Os outros 40% permitem uma política parcial, sendo que a organização fornece alguns dispositivos, mas permite que alguns dispositivos pessoais acessem sistemas corporativos.

Ainda de acordo com a Computer Word (2015), a mesma pesquisa relata que entre os motivos apontados para a não implantação do BYOD estão a necessidade de aprimoramento tecnológico (43%), a necessidade de centralizar o controle da segurança (35%) e a despreocupação dos usuários com segurança (31%).

Segundo Dodt (2012) uma complexidade do BYOD refere-se a sua visão holística, em que a utilização dos equipamentos dos funcionários dentro da empresa pode parecer muito simples e comum, mas na realidade, tudo dentro da organização está inteiramente interligado, e para melhor utilização com segurança, a TI e suporte interno têm que ser reestruturados para tal. Neste sentido, deve se investir mais em gastos em segurança da informação e infraestrutura e adequar a governança corporativa, políticas internas e trabalhar eficientemente em uma aculturação no local organizacional.

Em questão de segurança, Semola (2013) ressalta que funcionários terão sempre um cuidado extra utilizando seus próprios dispositivos tecnológicos para fins organizacionais, e como tanto a informação corporativa quanto dados pessoais se encontram no mesmo equipamento, a facilidade de uso do mesmo, tanto para buscar, manusear ou trabalhar alguma informação também aumenta, tornando a comunicação mais rápida e eficaz.

Dodt (2012) afirma que para uma real implantação de BYOD deve-se levantar várias informações que serão cruciais durante a reestruturação da empresa para este quesito, elas estão descritas a seguir no quadro 01:

Quadro 1 - Questionamentos iniciais para implantação de BYOD

Quais plataformas de dispositivos móveis devem ser suportadas?
Quais serviços corporativos esses dispositivos devem acessar?
Quais são os requisitos de segurança?
Existe alguma lei ou regulamentação que devo estar conforme?
Quais são as expectativas de privacidade de seus usuários?
Quais são as capacidades técnicas dos usuários?
Qual é o nível de suporte esperado?
O que é considerado “Aceitável” e “Inaceitável”?
Como será a política de reembolso de despesas?

Fonte: DODT (2012, p. 18)

Dodt (2012) sugere que para realizar uma implantação do BYOD em uma empresa, antes se deve realizar estudos e levantamentos através de um quadrante, onde é necessário analisar os pontos flutuantes nos eixos entre valor para o negócio e mitigação de riscos através das variáveis como restringir, permitir, abraçar e bloquear, descritas a seguir.

A variável restringir trabalha a questão de redefinir as políticas e procedimentos, tecnologia de apoio, arquitetura corporativa e por final definir níveis de suporte para tal. Já a variável permitir está relacionada à definição de políticas e procedimentos para uso, porém não prove suporte, e deve-se confiar no empregado (DODT, 2012).

Dodt (2012) ainda afirma que a variável abraçar trabalha a definição de políticas e procedimentos, efetua uma varredura por melhores práticas, implementa tecnologia de apoio, melhora a arquitetura corporativa e central de serviços corporativa.

Ainda segundo o autor citado anteriormente, no caso de bloquear; quando a terminologia de BYOD não irá possibilitar um diferencial e um melhoramento interno satisfatório, neste caso deve-se definir políticas e procedimentos para tal, além de definir controles técnicos para evitar a utilização e perca de desempenho dos funcionários, e trabalhar com monitoração para verificar se tudo está sendo seguido conforme as normas internas.

4 SEGURANÇA DA INFORMAÇÃO E BYOD

A Segurança da Informação é um assunto retratado mundialmente e se encontra em constante mudança e evolução, onde a informação a cada dia se torna um dos ativos mais valiosos para qualquer organização e deve ser muito bem trabalhada e armazenada. De acordo com Fontes (2012) pode-se traduzir segurança da informação como um conjunto de orientações, normas, procedimentos, políticas e demais ações que tem como principal objetivo proteger a informação e possibilitar que os negócios da organização sejam realizados e seus objetivos alcançados.

Semola (2013) menciona que a informação é um ativo que, como qualquer outro ativo importante, apresenta-se como essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida neste meio que está cada vez mais interconectado possibilitando que a informação esteja exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades.

Muitas empresas e organizações não possuem noção do valor de suas informações e não as protegem de maneira correta, o que proporciona riscos de perdas ou transmissões indevidas de dados sigilosos, possibilitando ocorrer prejuízos imensuráveis e em alguns casos a mesma pode vir a chegar à falência (FONTES, 2012).

A segurança da informação deve ser trabalhada à maneira e necessidade da empresa, e conta com algumas propriedades e requisitos principais para tal, que

incluem a integridade, disponibilidade, confidencialidade e autenticidade (SEMOLA, 2013).

Para este autor, o princípio de integridade prevê que a informação deve ser acessada somente por pessoas autorizadas. Segundo Campos (2007) integridade é quando a informação é confiável e possui garantia de que não houve alteração desde seu estado inicial de criação. Já a disponibilidade refere-se à garantia de que a informação ou meio tecnológico estará disponível para uso de pessoas autorizadas, sempre que necessário.

Considera-se como princípio de confidencialidade o fato de que a informação só poderá ser acessada ou compartilhada por pessoas autorizadas para tal; um dos métodos mais utilizados para quebrar este conceito é a engenharia social, que consiste em uma pessoa mal intencionada induzir outra a burlar regras e protocolos de segurança com objetivo de conseguir uma informação confidencial desejada (CAMPOS, 2007).

A autenticidade diz respeito à proteção das informações após o envio, garantindo que esta não seja modificada na comunicação e transmissão ao remetente, preservando também a identidade do remetente (SEMOLA, 2013).

Como o uso crescente no meio empresarial, principalmente dos tablets e smartphones, a maioria dos requisitos e recursos de segurança da informação estão interligados diretamente ao uso e controle do BYOD e consumerização organizacional. O acesso móvel sugere uma nova mentalidade, em que os dispositivos móveis e BYOD estão sujeitos a riscos de segurança e ataques presentes no mundo externo. Segundo Gilmore e Beardmore (2013, p. 14) os principais riscos à segurança destes dispositivos incluem:

- Perda de dados – como resultado de um dispositivo sendo perdido ou roubado.
- Roubo de identidade – se um criminoso roubar seu dispositivo e entrar nas suas contas online.
- Malware que rouba informações.
- Vazamento de informações, através de conexões Wi-Fi maliciosas.

O primeiro recurso para sanar tais vulnerabilidades se encontra na política de segurança da empresa, que deve ser adequada para esta evolução tecnológica e

acesso distribuído, a qual deve ser de fácil entendimento e claramente comunicada a todos os funcionários sem brechas para geração de dúvidas (DODT, 2012).

Taurion (2015) ressalta que toda política deve ser respeitada e o aspecto mais importante é tomar as ações necessárias para garantir que as violações de segurança simplesmente não aconteçam, caso contrário, medidas punitivas e saneadoras devem ser tomadas.

Com intuito de evitar problemas causados pela liberação do uso do BYOD e consumerização, empresas estão adotando soluções como o Gerenciamento de Dispositivos Móveis (Mobile Device Management – MDM), que se traduz como *softwares* administrativos que lidam com questões a respeito da incorporação de dispositivos móveis, como *tablets* e smartphones, em um ambiente corporativo, de forma segura e funcional, permitindo o controle e aplicação de regras no gerenciamento de políticas de segurança; configuração para dispositivos móveis; solução para prover conteúdo para usuários de acordo com seus papéis dentro da organização; e, disponibilização da segurança necessária para que informações sensíveis não sejam perdidas (GAJAR, 2013).

Cometti (2016) cita que uma solução MDM integrada ajuda a facilitar uma nova administração e tarefas de segurança em uma gama de diferentes dispositivos e Sistemas Operacionais (OS). A seguir no quadro 02, encontram-se descritas segundo o mesmo autor as principais funcionalidades das soluções oferecidas.

Quadro 2 – Funcionalidades de solução MDM

Mobile Device Management – que diz respeito a soluções para controle dos dispositivos móveis que estão sendo utilizados na empresa, permitindo total controle da empresa sobre o *hardware* do funcionário, o que engloba a realização de controles remotos no dispositivo, como por exemplo, deletar dados remotamente.
Workspace – que é a separação entre a parte da empresa, e do funcionário dentro do dispositivo, para que o funcionário possa utilizar seu dispositivo móvel e ter privacidade, quando não está trabalhando. Em resumo, diz respeito à separação clara dos dados pessoais do usuário e dos dados da empresa.
App Catalog – gerenciamento avançado das aplicações que usuário tem acesso em seu dispositivo móvel, havendo a possibilidade, por exemplo, de retirar uma aplicação de um celular remotamente.
E-mail – cliente de *e-mail* corporativo, controlado pela organização, mas que roda no dispositivo móvel do usuário.
Compartilhamento de Arquivos Corporativos – possibilidade de trocar arquivos corporativos através de um ambiente seguro da empresa dentro do dispositivo móvel do usuário, ou seja, o usuário pode ter acesso a arquivos de trabalho de maneira segura e em qualquer local.
Browsing – diz respeito à criação de navegadores customizados para dispositivos móveis, que são

monitorados e controlados remotamente pela empresa. Estes, por exemplo, podem abrigar aplicações de intranet.

Fonte: COMETTI, 2016

Segundo Dariva (2016) um programa BYOD mal implantado pode trazer mais problemas que soluções para a companhia, oriundos de acessos indevidos, roubo de informações e processos trabalhistas caso algo tenha que ser tratado judicialmente contra empregados ou terceiros.

A empresa Navita explica que cerca de 14 aspectos devem ser explorados e tratados, antes da implantação de um programa de BYOD, que são: entendimento da necessidade do cliente; entrevistas com os usuários-chave; mapeamento das políticas existentes; definição das políticas específicas para BYOD; mapeamento dos custos de mobilidade, já que nem sempre um programa de BYOD traz redução de custos; definição dos processos a serem implementados: projetos de MDM (*Mobile Device Management*) só devem entrar em operação após configuração de ferramentas, dispositivos, mas também da definição de todos os processos de suporte, atualização de ambiente, gerenciamento de apps, dentre muitos outros; definição da elegibilidade dos funcionários; definição dos dispositivos suportados; requisitos mínimos para escolha de ferramenta de MDM; definição do modelo de suporte BYOD a ser implementado; definição da política jurídica a ser assinada pelos colaboradores; definição de permissões e acessos; definição do plano de comunicação e processo de adesão; e estratégia de lançamento: como em qualquer projeto estratégico de TI ou mobilidade, a estratégia de lançamento deve ser cautelosa e liberar aos poucos os grupos de elegíveis(DARIVA, 2016).

5 CONSIDERAÇÕES FINAIS

BYOD é uma realidade que tende a crescer e evoluir, mas, também, surgirão novos desafios e problemas para o ramo empresarial. As organizações devem realizar uma análise de riscos para avaliar sua posição, a fim de extrair ao máximo os benefícios relacionados a este novo seguimento, para então adotar uma combinação de políticas claras, ferramentas adequadas de gestão da segurança das

informações aliados à reeducação dos usuários para o uso correto destas novas tecnologias e funcionalidades.

Fica claro que é importante a percepção pelas organizações que os funcionários utilizam cada vez mais inovações tecnológicas pessoais no ambiente de trabalho e devem inserir esta nova situação nas políticas de uso da informação, obtendo maior desempenho nos processos organizacionais e segurança.

As empresas não podem parar no tempo e abrir oportunidades de prospecção a suas concorrentes. Por isso, a questão de utilização de todos os novos modelos de dispositivos móveis juntamente ao seu desempenho e melhoria, tende sempre ao crescimento, e os setores de tecnologia devem ficar atentos às novas ameaças e oportunidades para alavancar sempre o uso eficaz e satisfatório dos mesmos.

REFERÊNCIAS

ANDERSON, J. Q.; RAINIE, L**. The future of the Internet III**. 2008.

CAMPOS, A. L. N. **Sistema de segurança da informação:** controlando os riscos. Santa Catarina: Visual Books, 2007.

CASTELLS, M. **Comunicaciónmóvil y sociedad**. una perspectiva global. Madri: Ariel/Fundación Telefónica. 2007. Disponível em: <http://www.eumed.net/libros/2007c/ 312/indice.htm>. Acesso em: 20 jan. 2016.

COMETTI, M. B.; AGUADO, A. G. Políticas de segurança da informação para BYOD. **Revista Tecnológica da Fatec Americana**, Americana, v. 4, n. 1, p.151-173, mar. 2016.

COMPUTERWORD. **Empresas estão abandonando o BYOD por "segurança", constata pesquisa.** Nov, 2015.

DARIVA, R. **14 Passos Para Seu Programa de BYOD Dar Certo**. Navita.

DODT, C. BYOD. O Novo Desafio para a Gestão de Risco Corporativa. In: **Global Risk Meeting**, 7º, 2012, São Paulo. Anais. São Paulo, 2012.

FALCÃO, D. Uso de Dispositivos Móveis. **Jornal Notaer,** Brasília, n. 06. junho de 2011.

FLEISHMAN, G. Empresas japonesas tornam indispensável uso do iPad. **Portal Nippo brasil Online,** 2010.

FONTES, E. **Políticas e normas para a segurança da informação:** como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações. Rio de Janeiro: Brasport, 2012.

GAJAR, P. K.; GHOSH, A.; RAI, S. Bringyourowndevice (BYOD): securityrisksandmitigatingstrategies. **Journalof Global Research in Computer Science**. v. 4, n. 4, apr. 2013.

GILMORE, G.; BEARDMORE, P. **Segurança Móvel e BYOD para leigos:** uma marca Wiley. Tradução de Kaspersky Lab. Inglaterra: John Wiley & Sons, 2013.

IDC Brasil. **Mercado brasileiro de PCs sofre queda de 36% nas vendas em 2015, segundo estudo da IDC Brasil**. São Paulo, 2016.

LEMOS, A. Comunicação e práticas sociais no espaço urbano: as características dos dispositivos híbridos móveis de conexão multirredes (DHMCM). **Revista Comunicação, Mídia e Consumo,** São Paulo, v. 4, n. 10, p. 23-40, 2007.

LOBO, F. **BYOD e consumerização:** conheça as diferenças e as semelhanças. Maio. 2013.

MILLER, S. K. Facingthe challenge of wireless security. **Journal IEEE Computer**, v. 34, p. 16-18, 2001.

RODRIGUES, C. Capitalismo informacional, redes sociais e dispositivos móveis: hipóteses de articulação. **Revista Galáxia**, São Paulo, n. 20, p. 70-83, dez. 2010.

SEMOLA, M. **Gestão da segurança da informação:** uma visão executiva. Rio de Janeiro: Elsevier, 2013.

SINGH, N. B.Y.O.D. genieis out ofthebottle – “devilorangel”.**Journal of Business Managemente & Social Sciences Research**. v. 1, n. 3, dez. 2012.

TAURION, C. **BYOD (bring your own device) na pratica**. 2015.

VIEIRA, B. **ComScore anuncia nova solução unificada do MMX™ multi-platform para mensurar audiências duplicadas Através de diferentes dispositivos no brasil**. São Paulo: ComScore, nov. 2015.