POLÍTICA DE SEGURANÇA PARA APLICAÇÃO BYOD

Débora Cocchi [1]
Eduardo Alves Moraes [2]

RESUMO

Este artigo tem por objetivo viabilizar o desenvolvimento de uma Política de Segurança para Aplicação BYOD, através da aprimoração de uma estratégia com o propósito de garantir o controle de acesso e uso seguro aos dados e sistemas organizacionais, objetivando solucionar as adversidades que este fenômeno traz às empresas.

Palavras-chave: BYOD. Controle de Acesso. Política de Segurança.

ABSTRACT

This article aims to make possible the development of a Security Policy for Application BYOD, by improving a strategy in order to ensure control of access and use secure data data and organizational systems, aiming at solving the odds that this phenomenon brings to companies.

Keywords: BYOD. Access Control. Security Policy.

RESUMEN

Este articulo tiene como objetivo viabilizar el desarrollo de uma Politica de Seguridad para Aplicación BYOD, a traves de la aprimoración de uma estratégia com el proposito de assegurar el control del aceso y uso seguro a los dados y sistemas organizacionales, objetivando solucionar las adversidads que este fenómeno trae para las emplecias.

Palabras-Llave: BYOD. Control del Aceso. Politica de seguridad.

[1] Estudante do Curso Análise de Sistemas e Tecnologia da Informação – FATEC – Campus Ourinhos/SP.
E-mail: debora_cocchi@hotmail.com

[2] Professor Orientador: Esp. Eduardo Alves Moraes – FATEC – Campus Ourinhos/SP. E-mail: eduardo.moraes@fatec.sp.gov.br

Introdução

No ranking de investimento em novas tecnologias quem sai na frente é o consumidor final, uma vez que ele possui acesso fácil a essas mudanças e faz questão de possuir as mais atuais novidades do ramo tecnológico. Já para as corporações, devido a esta instabilidade e variedade que o mercado oferece torna-se difícil prover uma tecnologia de ponta e atualizada. Elementos estes, determinantes na expansão da consumerização em TI, que incentivaram o movimento Bring Your Own Device (BYOD), ou seja, "traga seu próprio dispositivo".

O BYOD prega uma maior flexibilidade aos profissionais para que possam utilizar seus dispositivos móveis pessoais também no ambiente de trabalho.

Fator que possui seus prós e contras, afinal, para a empresa é viável não ter que gastar com um grande número de equipamentos e ainda ter que mantê-los atualizados. Para o funcionário seria uma inovação possuir o dispositivo atual com as mais novas tecnologias de software e hardware do mercado também no ambiente corporativo.

Entretanto, como a parte de TI controlaria o acesso a informações confidenciais da empresa em tantos SmartPhones, Androids, tablets, notebooks, iPhones ,iPads e suas tecnologias em toda a empresa? Já os profissionais que optarem por utilizar seus próprios dispositivos, como garantir que a corporação não tenha acesso a seus dados privados?

Visualizando esta circunstância, não tem como deixar de lado a suma importância do controle de acesso destes dispositivos em toda a empresa. Entretanto, há quem acredite que a melhor forma de controlar essa situação seja proibindo o uso desses aparelhos. Contudo, sabe-se que é improvável o sucesso desta conduta.

Segundo o coordenador de pesquisas da IDC Brasil apud Olhar Digital,

> O mercado está mudando mais rápido e as empresas que forem inflexíveis podem ter problemas com os funcionários, que ficarão desmotivados. É importante pensarmos da seguinte forma: se não podemos impedir essa transformação, devemos tirar proveito dela (CRIPPA, 2012 apud OLHAR DIGITAL, 2012).

Desta forma, cabe ao TI desencadear medidas de segurança para aplicação BYOD focando no controle de acesso, de forma a ajustá-las de acordo com a necessidade dos serviços a serem desenvolvidos, atender os princípios da empresa e proporcionar condições efetivas para que o funcionário possa executar a atividade com o seu próprio dispositivo.

O presente artigo tem como finalidade demonstrar a importância da elaboração de uma estratégia de BYOD que defina uma política para acesso e uso seguro aos dados e sistemas da organização, visando solucionar o problema que a maioria das empresas encontram em administrar o uso desses dispositivos.

Conhecendo o fenômeno BYOD

O mercado está mudando de forma repentina, mal acostumamos com uma tecnologia e logo surge outra. O que faz com que cada vez mais o usuário final esteja à frente das organizações, neste quesito, trazendo à tona o fenômeno Bring Your On Device (BYOD).

De acordo com o editor executivo da InfoWorld, poucas tendências tecnológicas impuseram o seu caminho para o mundo empresarial tão rapidamente quanto o BYOD.

> O movimento começou timidamente em 2007 com o lançamento do iPhone mas ganhou força em meados de 2010, quando a Apple adicionou funcionalidades corporativas e de gestão e recursos de segurança no iOS 4. Um ano mais tarde, as políticas nas TIs de não autorizar a conexão dos dispositivos na rede da empresa estavam em frangalhos, com a maioria das empresas adotando o BYOD para uma parte dos seus empregados e para os dispositivos iOS (GRUMAN, 2012).

Segundo o Olhar Digital (2012), o BYOD "tem sido visto com bons olhos pelos recrutadores". O mesmo ainda cita um relatório da Cisco Horizons IBSG, que contou com mais de 600 líderes do mercado de TI e de negócios dos Estados Unidos, onde foi observado que 95% das organizações já concedem aos colaboradores levarem seus dispositivos ao local de trabalho. Ainda, "84% fornecem algum tipo de apoio técnico ou funcional, e 36% oferecem suporte completo para qualquer aparelho que o empregado traz para o ambiente profissional" (Olhar Digital, 2012).

Conforme Junior (2012) apud Olhar Digital (2012), gerente de desenvolvimento de negócios de Borderless Networks da Cisco - Brasil,

> O BYOD tem sido aceito aqui no País pela alta gerência de grandes corporações. No entanto, o mercado brasileiro ainda carece de uma infraestrutura adequada, e a solução está na mobilidade - em especial na cobertura Wi-Fi. Imagine gerenciar os semáforos com esse tipo de conexão, por exemplo. A longo prazo, isso vai melhorar nossa qualidade de vida e dar ao governo a oportunidade de renovar o país e nossa cultura (JUNIOR, 2012 apud OLHAR DIGITAL, 2012).

Bradley (2011), colunista na Revista PC World/EUA e autor do blog Net Work, afirma que "Há uma variedade de benefícios em permitir que os usuários forneçam seu próprio PC e dispositivos móveis, mas há também algumas preocupações".

Por um lado, o mesmo, afirma que as "Empresas que abraçam o BYOD têm algumas vantagens sobre as concorrentes" (BRADLEY, 2011). Nestas circunstâncias, o aspecto financeiro tem sido bastante atraente, afinal "Com o trabalhador pagando a maioria dos custos de aquisição do hardware, e dos serviços de voz e dados, além de outras despesas associadas, as empresas economizam muito dinheiro" (BRADLEY, 2011). O colunista diz que segundo estudos, nos Estados Unidos, as empresa estimam uma economia de 80 dólares mensais por usuário. Avaliando

esta situação, pode-se esperar que os colaboradores que utilizam a tecnologia não estejam satisfeitos em arcar com todos os gastos, uma vez que o utilizam para o trabalho. Contudo, segundo Tony (2011), "Muitas empresas americanas estão exigindo que os funcionários cubram todos os custos - e eles estão felizes em fazê-lo". Alem do que, "Os profissionais se sentem mais à vontade e produtivos porque podem usar os dispositivos que preferem, e não os que estão disponíveis dentro do ambiente de trabalho" ressalta Junior (2012) apud Olhar Digital (2012), e explica:

> com cada funcionário utilizando os dispositivos trazidos de casa, os únicos custos seriam apenas os de manutenção da conta de cada pessoa e não de uma base de vários desktops - isso sem contar a possbilidade de um trabalho mais dinâmico graças a mobilidade. Para os empregados, isso traz mais facilidade na hora de desempenhar suas tarefas diárias com seus aparelhos de uso pessoal e atende melhor as necessidades em nível corporativo, colaborando mais e aumentando a produtividade (OLHAR DIGITAL, 2012).

Em contrapartida, Messmer (2012), editora sênior da Network World/EUA, diz que embora a empresa não tenha custos com a aquisição de novos dispositivos móveis e estabeleça um ambiente de trabalho mais amigável, há um aumento de custos com a manutenção destes equipamentos, alegando que os custos com help desk não caíram.

Através de uma pesquisa realizada com 116 companhias de TI e Telecom, foi confirmado que "Mais de dois terços (70%) responderam que não viram ainda nenhuma mudança com BYOD, mas 28% disseram que os custos aumentaram em 20%" (MESSMER, 2012). Verificou-se ainda não ser esperado por parte do profissional que utiliza seu próprio equipamento um apoio técnico da TI. Entretanto, conforme Messmer, "as empresas estão dispostas a ajudá-los a resolver problemas de conectividade e degradação dos aparelhos".

Entre os pontos positivos citados por Tony Bradley (2011), encontra-se o fator de atualização de hardware, que é realizada de forma mais contínua do que os "ciclos de refresh dolorosamente lentos da maioria das organizações".

Crippa (2012) apud Olhar Digital (2012), lembra algumas preocupações por parte de muitos líderes, tais como o aumento de distração, devido os profissionais poderem "jogar apps ou checar redes sociais enquanto trabalham", além de questões de segurança, onde a pesquisa aponta que "19% acreditam que gastarão drasticamente com o investimento de plataformas de segurança para os novos dispositivos", enquanto que

> 83% dos profissionais temem a falta de segurança da informação nestes dispositivos, 56% se preocupam com vírus que podem ser adquiridos nas redes sociais e 52% acreditam que será um imenso desafio desenvolver uma nova política corporativa para acompanhar a tendência (OLHAR DIGITAL, 2012).

Diante destas circunstancias, há o grande desafio de como o administrador de TI irá salvaguardar os sistemas e manter o controle da sua rede.

Vale lembrar que a TI deve repensar suas políticas de adoção de novas tecnologias, sem ignorar o fato de que o BYOD já é uma realidade. Recomenda-se buscar uma relação hamônica entre as partes, implementando o controle de acesso em uma Política de Segurança para Aplicação BYOD, de forma a garantir o resguardo do usuário (empresa/ funcionário) desta tecnologia.

Como gerenciar essa tendência?

Cada vez mais é comum ver profissionais lendo e-mails do trabalho e acessando os sistemas das empresas a partir de seus próprios dipositivos (OLHAR DIGITAL, 2012). Entretanto, "'Há quatro ou cinco anos, o uso dos dispositivos móveis era restrito a um grupo de elite'", lembra Herrema (2012) apud Olavsrud (2012). Segundo ele, "os aparelhos eram mais usados para acesso de aplicações básicas como e-mail". Todavia, hoje, com o BYOD, esses equipamentos acessam vários sistemas organizacionais.

"O aumento do consumo desses dispositivos no ambiente corporativo gera um certo temor para empresas, preocupadas com perda de dados", afirma Olavsrud (2012), escritor sênior da CIO.com. Nestas condições, percebe-se a necessidade da implementação do controle de acesso à rede, de modo a proteger as informações da organização.

De acordo com o estudo da Avanade (2012), provedora de soluções de negócios de tecnologia e serviços gerenciados, baseado em uma pesquisa realizada com empresas de diversos ramos, em 17 países, contando com o Brasil, e com mais de 600 líderes seniores e de TI, verificou-se que 88% dos executivos informaram que os funcionários já usam seus próprios equipamentos para fins profissionais.

No Brasil, segundo o estudo, a utilização de tecnologias de computação pessoal no ambiente corporativo para fins comerciais é maior do que em vários países europeus, alcansando 97% e também que os Estados Unidos (89%).

Essa iniciativa dos profissionais levarem seus próprios aparelhos para utilizarem no serviço ocorre porque, conforme Crippa (2012) apud Olhar Digital (2012), os funcionários encontram-se insatisfeitos com os dispositivos que as empresas disponibilizam a eles:

> Em geral as companhias substituem suas tecnologias de quatro em quatro anos, mas para algumas pessoas este período pode ser longo demais, principalmente, se elas são ligadas em tecnologia e possuem em casa dispositivos mais modernos e melhores (CRIPPA, 2012 apud OLHAR DIGITAL, 2012).

Diante desta situação, fica evidente que não há mais como evitar esta tendência, "a questão deixou de ser 'permitir ou não permitir', e passou a ser 'como gerenciar esse mar de aparelhos'"

(SOARES, 2012), " desafiando assim os gestores de segurança e tecnologia da informação a pesquisarem soluções capazes de suportar suas necessidades de negócio e os pré-requisitos adequados da segurança", diz Ferreira e Araújo (2008, p.103).

Os mesmos ainda dizem que algumas questões são levantadas neste cenário:

- Como se conectar remotamente de forma segura?
- Como assegurar que o usuário correto está acessando a informação correta?
- Como controlar o uso indiscriminado de eventuais dispositivos para o acesso remoto?

De acordo com a ISO/ IEC 27001:2005, que salienta técnicas de segurança da informação, deve-se tratar os riscos através de controles visando reduzir as chances da ocorrência de um impacto danoso (SANTOS, 2012). Para isso é fundamental a empresa obter um controle de acesso efetivo dos dados corporativos que os profissionais estão manuseando em seus dispositivos.

> Como regra geral, o acesso deve ser concedido levando em conta a função desempenhada pelo colaborador. As autorizações e aprovações necessárias para o cumprimento dos procedimentos e instruções de trabalho devem ser fornecidas conforme a hierarquia de responsabilidades (FERREIRA; ARAÚJO, 2008, p.90).

O gerente de desenvolvimento de negócios da Multirede (2012) lembra que há instrumentos de controle de acesso que detectam quem está acessando a rede, onde e qual o tipo de computador esta sendo utilizado. E fala sobre alternativas de MDM (*Mobile Device Management*), que é um meio de controle focado em dispositivos móveis, tornando-se "um grande aliado dos administradores de rede para aplicação de políticas de segurança de acordo com as características de cada tipo de acesso para smartphones e tablets" (SANTOS, 2012). Outra alternativa que o gerente aponta é a virtualização:

> O dispositivo móvel acessa um servidor no qual as informações são processadas, não havendo necessidade de armazenamento local. Todas as informações e aplicações ficam no servidor corporativo. Outro recurso já disponível é a possibilidade de apagar remotamente os dados ou aplicações em um dispositivo móvel, seja por erros de senha, aplicação modificada ou por comando remoto do administrador de forma centralizada" (SANTOS, 2012), explica.

Segundo Gartner (2012) apud Messmer (2012), a difusão do BYOD vai impulsionar o resurgimento do NAC (*Network-Acess Control*), controle de acesso baseado em política de segurança, que ocorreu há dez anos, contudo na época o gerenciamento dos terminais não eram tão desenvolvidos, o que fez com que ele não fosse tão apreciado (MESSMER, 2012). No entanto, Orans (2012) apud Olhar Digital (2012), afirma que, agora, o NAC junto com o MDM devem ganhar popularidade devido o aumento da consumerização que passa a exigir mais segurança para os dispositivos móveis.

De acordo com Gartner (2012) apud ForeScout (2012), o NAC oferece a flexibilidade que as companhias necessitam em um ambiente BYOD, ao fornecer meios que possibilitam o controle sobre a rede.

Empresas como a IBM, Cisco e HP também oferecem soluções que permitem o gerenciamento de forma simples e segura dos dispositivos que os profissionais utilizam nas empresas (OLHAR DIGITAL, 2012). "As aplicações criptografam dados, monitoram e controlam as informações remotamente e podem realizar bloqueio de dados caso os dispositivos sejam roubados ou perdidos" (OLHAR DIGITAL, 2012).

Vale lembrar que "A organização deve somente disponibilizar recursos tecnológicos aos colaboradores (funcionários e terceiros) autorizados de modo a auxiliá-los no desempenho de suas funções e na execução dos trabalhos" (FERREIRA; ARAÚJO, 2008, p.87), ou seja, as permissões devem ser estabelecidas de acordo com a função desenvolvida.

De acordo com Ferreira e Araújo (2008, p. 87), deve constar na política "que cada colaborador é responsável por usar os recursos tecnológicos disponíveis de forma a aumentar sua produtividade e contribuir para os resultados e a imagem pública da organização".

A partir da análise desses dados percebe-se a grande importância de estabelecer um meio de gerenciamento dos profissionais que acessam a rede e os sistemas corporativos através de seus dispositivos, visando garantir a segurança da informação. Afinal, a "'solução está na rede, e não no dispositivo'" (JUNIOR, 2012 apud OLHAR DIGITAL, 2012).

Política de Segurança para Aplicação BYOD

Sabe-se que a consumerização é uma realidade e tentar proibir o fenômeno BYOD não é a melhor opção, afinal, com ou sem a permissão da empresa, os usuários descobrirão um meio de acessar o sistema através de seus próprios aparelhos. Sendo assim, esta questão deve ser administrada de forma sensata,

> a área de TI deve desenhar estratégias de convivência, que permitam ao mesmo tempo, oferecer dentro das empresas experiências similares a que os funcionários têm em casa, mas que garantam um nível de segurança adequado aos seus requisitos de compliance e auditoria corporativos (Taurion, 2012).

Para isso, uma Política de Segurança para Aplicação BYOD deve ser estabelecida, onde será definido critérios de aceitação para o uso de dispositivos móveis particulares no ambiente corporativo. É importante elaborar esta Política de forma que ela seja completa sem ser complexa, ou seja, ela "deve ser simples o bastante para que todos na organização compreendam o porquê e a forma de conduzir suas atividades do dia-a-dia, alinhadas às práticas seguras e sintonizadas com a

proteção das informações da organização" (FÁVERO, 2008 apud FERREIRA; ARAÚJO, 2008, p. XVI).

As áreas de gestão de risco, jurídicas e de recursos humanos também devem ser envolvidas neste processo, afinal aspectos legais e trabalhistas estarão inclusos neste meio (TAURION, 2012).

Vale lembrar que a Política de Segurança para Aplicação BYOD é um meio da empresa e do profissional responsável pelo gerenciamento de TI estar se resguardando, caso o usuário faça mal uso de suas permissões, infringindo as regras propostas. Mas para isso, é necessário que os funcionários assinem um termo de ciência da Política aplicada, se comprometendo a cumprí-la. Para que ela seja bem sucedida, Ferreira e Araújo (2008, p. 44), citam alguns itens muito relevantes:

- Formalização dos processos e instruções de trabalho;
- Utilização de tecnologias capazes de prover segurança;
- Atribuição formal das responsabilidades e das respectivas penalidades;
- Classificação das informações;
- Treinamento e conscientização constantes.

Para definir uma Política de Segurança para Aplicação BYOD, deve-se estabelecer alguns critérios. Segundo o gerente de novas tecnologias da IBM Brasil, o primeiro passo é definir a estatégia:

> valide se existem restrições legais, implicações nos aspectos relacionados com remuneração dos funcionários e obtenha aval da auditoria e da área de gestão de riscos. Uma empresa global tem que entender que uma política única nem sempre poderá ser aplicada, uma vez que as legislações e as culturas são diferentes entre os países que atua (TAURION, 2012).

Para evitar possíveis problemas futuros, deve-se deixar bem claro na Política de Segurança para Aplicação BYOD:

- Objetivo do Programa BYOD:

  De acordo com Taurion (2012), "deve-se definir claramente os objetivos do programa e justificar seu business case", ou seja, explicitar os benefícios a serem alcansados e se "serão intangíveis, como melhoria da imagem" ou se "poderão ser mensurados, como aumento da produtividade", explica.

- Amplitude do Programa:

  Taurion (2012) explica que deve ser estabelecido se a adesão do programa será obrigatória - se sim, a empresa deve definir se irá adquirir equipamentos para os funcionários que não desejam fazer parte do programa, tendo em vista que os profissionais que disponibilizaram

seu dispositivo poderão ver esta atitude como um benefício aos que não quiseram participar da proposta da empresa.

Também deve ser especificado quem participará do programa - "todos os funcionários ou apenas uma parcela especifica" (TAURION, 2012).

- A propriedade do equipamento:

  De acordo com Taurion (2012), há três formas de abordar esta questão.

> A primeira é estabelecer que se os recursos corporativos forem acessados por um dispositivo pessoal, a empresa tem o direito de controlar e bloquear o aparelho. [...] No segundo modelo, a empresa compra o dispositivo e permite seu uso para fins particulares, além, óbviamente das atividades profissionais. [...] O terceiro modelo é a transferência legal do dispositivo para o funcionário, que pode ser, em alguns casos, permanente. Mas há também a situação em que a organização compra o aparelho por um valor simbólico e dá ao profissional o direito de usá-lo para fins pessoais, comprometendo-se a vendê-lo de volta pelo mesmo preço quando o empregado deixar a empresa (TAURION, 2012).

- Quem vai arcar com os custos das ligações:

  É importante definir se os custos com ligações e acesso a dados serão reembolsados pela empresa. Em caso positivo, se será total ou parcial. Taurion (2012) explica que "muitas empresas reembolsam os funcionários que usam o seu próprio dispositivo particular nas atividades profissionais, pagando os custos das chamadas e do acesso a dados. Outras cobrem metade das despesas, mediante apresentação de relatório dos gastos".

- Os requitos de segurança que devem ser cumpridos:

  É fundamental "educar os funcionários quanto a política, restrições e riscos envolvidos" (TAUION, 2012) nesta adoção e a importância do cumprimento das condições propostas.

  De acordo com a IDGNOW (2012), deve-se esclarecer na Política que o usuário será responsável pelo equipamento, assim como pelo conteúdo armazenado no mesmo. Além de estar ciente e concordar que o dispositivo "estará sujeito a monitoramento e a inspeção física por parte da empresa" (IDGNOW, 2012).

  Ressalta ainda a questão de softwares que devem possuir licença para evitar que a empresa seja envolvida em um incidente de pirataria, devido o equipamento estar sendo utilizado em prol da organização. "Por conta disso, muitas empresas tratam do cenário de forma híbrida, onde o equipamento é do usuário mas a camada de softwares é fornecida pela empresa, de modo a tentar mitigar riscos com pirataria" (IDGNOW, 2012), explica.

  Esta questão deve constar na Política de Segurança para Aplicação BYOD, de forma que o usuário declare que os softwares em seu equipamento utilizados para fim corporativo

"possuem licença regular sob pena de responder isoladamente sobre qualquer incidente de pirataria" (IDGNOW, 2012).

Deve-se aboradar, também, o comprometimento do profissional em "realizar backup de todas as informações pertinentes à empresa e de salvá-las na rede corporativa" (IDGNOW, 2012).

Outra questão que não pode deixar de ser abordada, lembra Taurion (2012), são os procedimentos que deverão ser realizados quando o funcionário deixar a empresa. Estas instruções devem ser bem definidas para evitar possíveis problemas como a perda de informações.

- Permissões de acesso:

Segundo Taurion (2012), os profissionais devem ser associados de acordo com utilização e demanda para os dispositivos. "As atividades profissionais em uma empresa são bem diversas e, consequentemente, as suas demandas de uso tendem a ser bem diferentes" (TAURION, 2012), o que leva a estabelecer permissões de acesso ao sistema distintas, afinal, não é necessário nem viável o profissional da área comercial ter acesso ao sistema que contém os dados cadastrais dos funcionários, por exemplo.

Para auxiliar neste quesito, Taurion (2012) sugere a construção de "uma matriz de funções efetuadas versus demandas de aplicações e usos".

- Questão jurídica:

É um elemento muito importante a ser tratado por ser o meio que garantirá o resguardo da empresa em possíveis ações processuais.

IDGNOW (2012), alerta para questões trabalhistas em consequência da alteração do artigo 6º da CLT – Consolidação das Leis do Trabalho. E destaca que deve ser previsto na Política que "o mero acesso ou uso do equipamento ou recursos de informação pelo proprietário, por si só, não configura sobreaviso ou sobrejornada, sendo um ato de liberalidade, proatividade e iniciativa do mesmo".

Além do que, deve constar que:

> o equipamento está sendo colocado à disposição da empresa como beneficiária de uso temporário e parcial, em caráter não oneroso, sem qualquer responsabilidade por parte da empresa; [...] a empresa não se responsabiliza pela perda, deterioração, furto, extravio, quebra do equipamento, e se isso vier a ocorrer o proprietário deverá avisar a empresa imediatamente; [...] o proprietário compromete-se a portar o equipamento de forma discreta e com o máximo de zelo possível, para evitar incidentes e vazamentos de informação da empresa (IDGNOW, 2012).

Vale lembrar, que se na Política de Segurança para Aplicação BYOD constar que é de responsabilidade do proprietário do dispositivo móvel realizar a sua manutenção e a empresa vier a prestar estes serviços que deveriam ser feitos pelo funcionário "acabará atraindo para si todo o ônus de zelo do bem, gerando riscos legais em sua política de BYOD" (IDGNOW, 2012).

De acordo com Taurion (2012), após estabelecer todos estes critérios, deve-se começar a executar o projeto BYOD.

> Isto envolve um planejamento detalhado das etapas a serem cumpridas, o processo de educação, a criação e formalização da política de uso, o treinamento e operação das novas atividades dos funcionarios do help desk e a aquisição e instalação das tecnologias necessárias à gestão dos processos (TAURION, 2012).

O mesmo ainda diz que o teste deve ser realizado em um projeto piloto, onde será feito ajustes e os procedimentos refinados, a partir daí o BYOD deverá ser disseminado pela empresa. "É a etapa do rollout", explica Taurion.

É importante lembrar que um fator determinante para o sucesso dessa medida é manter a Política sempre válida e atualizada (IBM, 2012).

A partir da análise destes princípios, conclui-se que a Política de Segurança para Aplicaçao BYOD é essencial para que a empresa estabeleça de modo formal as condições para que os profissionais possam utilizar seus equipamentos móveis no ambiente corporativo sem comprometer a segurança da informação, além de, em caso do descumprimento de alguma destas orientações, a organização ter como requerer seus direitos.

CONCLUSÃO

A partir da análise desses dados é possível perceber que, por ser um conceito inovador, o BYOD ainda não deixa uma ideia clara de até onde pode ser considerado positivo ou negativo. Entretanto, o que se sabe é que este movimento chegou para ficar e não adianta tentar bloqueá-lo.

Diante destas circunstancias, há o grande desafio de como o administrador de TI irá salvaguardar os sistemas e manter o controle da sua rede.

Sendo assim, verifica-se a grande importância de estabelecer um meio de gerenciamento dos profissionais que acessam a rede e os sistemas corporativos através de seus dispositivos, visando garantir a segurança da informação. Para isso, recomenda-se implementar o controle de acesso em uma Política de Segurança para Aplicação BYOD, de forma a garantir o resguardo do usuário (empresa/ funcionário) desta tecnologia.

Logo, conclui-se que a Política de Segurança para Aplicaçao BYOD é essencial para que a empresa estabeleça de modo formal as condições para que os profissionais possam utilizar seus equipamentos móveis no ambiente corporativo sem comprometer a segurança da informação.

REFERÊNCIAS

AVANADE. **Pesquisa global da Avanade revela o comportamento e dissipa mitos da Consumerização de TI**. Disponível em: <http://www.avanade.com/pt-br/about/avanade-news/press-releases/Documents/Avanade_PR_CoIT_Brazil_Ptg.pdf>. Acesso em: 12 nov. 2012.

BRADLEY, Tony. **Prós e contras do BYOD**. Disponível em: <http://cio.uol.com.br/gestao/2011/12/22/pros-e-contras-do-byod/>. Acesso em: 20 set. 2011.

SOARES, Edileuza. **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: 20 set. 2012.

FERREIRA, F.N.F; ARAÚJO, M.T. **Política de Segurança da Informação – Guia Prático para Elaboração e Implementação**. 2. ed. Rio de Janeiro: Ciência Moderna, 2008.

FORESCOUT. **BYOD Security**. Disponível em: <http://www.forescout.com/solutions/byod/>. Acesso em: 15 nov. 2012.

GRUMAN, Galen. **A Era BYOD pode estar no começo do fim**. Disponível em: <http://cio.uol.com.br/gestao/2012/04/24/a-era-byod-pode-estar-no-comeco-do-fim/>. Acesso em 29 out. 2012.

IBM. **A vez do BYOC (Bring Your Own Cloud)**. Disponível em: <https://www.ibm.com/developerworks/mydeveloperworks/blogs/ctaurion/entry/a_vez_do_byoc_%28bring_your_own_cloud%29?lang=en>. Acesso em: 29 out. 2012.

IDGNOW. **Evite riscos com a política de BYOD**. Disponível em: <http://idgnow.uol.com.br/blog/digitalis/2012/10/11/evite-riscos-com-a-politica-de-byod/>. Acesso em: 12 nov. 2012.

MESSMER, Ellen. **BYOD resgata conceito de controle de acesso à rede**. Disponível em: <http://computerworld.uol.com.br/tecnologia/2012/05/09/byod-resgata-conceito-de-controle-de-acesso-a-rede/>. Acesso em: 20 set. 2012.

MESSMER, Ellen. **Empresas buscam modelo para reembolso do BYOD**. Disponível em: <http://cio.uol.com.br/gestao/2012/07/25/empresas-buscam-modelo-para-reembolso-do-byod/>. Acesso em: 20 set. 2012.

OLAVSRUD, Thor. **Consumerização: Como manter a segurança dos dispositivos móveis**. Disponível em: <http://cio.uol.com.br/gestao/2012/08/10/consumerizacao-como-manter-a-seguranca-dos-dispositivos-moveis/>. Acesso em: 20 set. 2012.

OLHAR DIGITAL. **"Bring your own device": como as empresas estão encarando a consumerização de TI**. Disponível em: <http://olhardigital.uol.com.br/imprimir/negocios/digital_news/noticias/como-as-empresas-estao-encarando-a-consumerizacao->. Acesso em 01 set. 2012.

OLHAR DIGITAL. **Bring your own device: que tal levar seus próprios dispositivos para o trabalho?**. Disponível em: <http://olhardigital.uol.com.br/produtos/mobilidade/noticias/bring-your-own-device-que-tal-levar-os-proprios-dispositivos-para-trabalhar>. Acesso em 01 set. 2012.

SANTOS,Tácito. **BYOD, como controlar dispositivos móveis nas empresas?**. Disponível em: <http://olhardigital.uol.com.br/imprimir/negocios/seguranca/noticias/byod%2c-como-controlar-dispositivos-moveis-nas-empresas>. Acesso em: 01 set. 2012.

TAURION, Cezar. **A consumerização é o próximo desafio da área de TI**. Disponível em: <http://imasters.com.br/artigo/25225/gerencia-de-ti/a-consumerizacao-e-o-proximo-desafio-da-area-de-ti>. Acesso em 29 out. 2012.

TAURION, Cézar. **BYOD (Bring Your Own Device) na prática**. Disponível em: <http://www.ibm.com/midmarket/br/pt/articles_byod_como_comecar.html>. Acesso em: 19 nov. 2012.