O Uso de Gadgets Pessoais no Trabalho e o Impacto na Segurança Corporativa e na Gestão de Pessoas: a Consumerização de Ti

Ricardo Alves Said
rasaidvr@yahoo.com.br
AEDB

Paulo Eduardo Oliveira Gimenez
prof.gimenez@ig.com.br
UBM

Gláucia Araújo Lima
glaucia.araujo.adm@bol.com.br
FaSF

Márcia Aparecida de Oliveira
marcia.oliveira@grupoapereira.com.br
FaSF

Resumo:O avanço tecnológico está fazendo com que as organizações se adequem às novas formas de trabalho para se manterem no atual mercado competitivo. Para auxiliar as empresas na conquista de novas estratégicas mercadológicas, surge à tendência da Consumerização de TI a qual está revolucionando a forma de trabalho dentro das organizações. Esta tendência permite que o funcionário trabalhe com seu gadget pessoal. Ao mesmo tempo em que a Consumerização é positiva aos resultados operacionais, riscos à segurança da informação corporativa podem surgir e problemas de ordem trabalhista devem ser considerados para a implementação eficaz desta metodologia. Assim este artigo tem o objetivo de analisar os riscos gerados na segurança da informação corporativa com a prática desta tendência e o que a CLT aborda sobre esse tema. A metodologia abordada neste estudo foi a pesquisa de campo realizada com profissionais de RH e TI de três organizações, como forma de verificar o grau de conhecimento, aceitação, interesse e prática na organização em que atuam sobre o tema. Pode-se constatar um alto grau de maturidade em relação a essa prática na visão dos gestores, que exige uma adequação da suas políticas de segurança da informação para a utilização desta prática inevitável entre os funcionários e o negócio atualmente.

Palavras Chave: Consumerização - BYOD - Gadget - Tecnologia -

1. INTRODUÇÃO

Uma nova tendência que envolve tecnologia de uso pessoal vem sendo adotada pelas organizações e ao mesmo tempo, revolucionando a forma de atuação diária do trabalhador de escritório. Essa prática é conhecida pela sigla *BYOD* o que significa *Bring Your Own Device* (Traga Seu Próprio Dispositivo) ou pelo termo Consumerização nos Negócios. Em outras palavras, consiste no modelo em que o funcionário leva seu dispositivo pessoal para o trabalho como, por exemplo, smatphones, tablets ou notebooks, e exerce suas atividades com o auxílio destes *Gadgets*.

Observa-se que a adoção desta tendência pelas organizações acarreta em grande vantagem competitiva por permitir um aumento de produtividade no trabalho, e também, riscos preocupantes. Sendo assim, surge uma questão, até que ponto é vantajoso uma organização adotar este modelo de negócio, autorizando seu colaborador a utilizar seu dispositivo pessoal com finalidade profissional?

O funcionário no BYOD sente-se motivado e adquire um dispositivo eletrônico que venha agregar mais afinidade e melhor execução de suas atividades, e com isso, a empresa eleva seus índices de produtividade e diminui seu investimento em compras ou *upgrades* de dispositivos para seus funcionários. Ao mesmo tempo, o BYOD obriga a organização a desenvolver e praticar uma excelente estratégia, a qual deve contemplar uma Política de Segurança de Informação bem elaborada e que envolva inclusive questões trabalhistas.

Este trabalho tem como objetivo analisar os riscos à Segurança da Informação com a prática da Consumerização ou *BYOD* na cultura organizacional, bem como avaliar se a Consolidação das leis do trabalho - CLT nacional já caracteriza esta prática e relacionar as alternativas de segurança e controle para o sucesso da implementação deste método.

Se uma empresa pratica a Consumerização, e o seu funcionário trabalha com seu próprio *Gadget*, a empresa obtém como resultado otimização de tempo, recursos e redução de gastos relacionados a tecnologia da informação. Se a mobilidade for permitida ao profissional, o colaborador se tornará motivado em exercer sua função com conforto e praticidade cujo desenvolvimento das suas atividades laborais torna-se-a mais produtiva e prazerosa.

A metodologia a ser adotada na elaboração deste artigo científico aborda a pesquisa de campo, que consiste na observação de fatos e fenômenos exatamente como ocorrem na realidade, na coleta de dados referentes aos mesmos e na análise e interpretação desses dados, fundamentando-se na teoria consistente, objetivando a compreensão e explicação do problema em evidência. Através deste método, viabiliza-se agrupar em uma única base de dados todas as informações coletadas, baseando-se também em pesquisa bibliográfica, quantitativa e qualitativa exploratória.

Este trabalho foi dividido em três capítulos, sendo o primeiro capítulo intitulado como "A expansão da utilização dos *Gadgets* para fins diversos e sua relação com a Consumerização", onde foram aprofundados os temas: Conceitos de *Gadgets*; o uso dos *Gadgets* para fins pessoais e profissionais; e o Conceito de Consumerização ou *BYOD*. O segundo capítulo com o tema "A Consumerização pela ótica da Segurança da Informação" aborda o "Conceito de Segurança da Informação, a "Consumerização: riscos e recomendações; e a Consumerização: pontos positivos." O terceiro capítulo intitulado como "Os profissionais de Gestão de Pessoas e Gestão de TI e a Consumerização: Pesquisa de Campo" inicia-se com o tópico "As Leis Trabalhistas e a Consumerização", que destaca posteriormente, o que reza a CLT sobre este tema. Ainda no capítulo três, em um segundo momento é apresentado como esta tendência é abordada por três gerentes de Gestão de

Pessoas e Gestão de TI, de instituições organizacionais distintas, situadas na cidade de Volta Redonda, através de pesquisa de campo, finalizando assim, com uma análise crítica.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. A EXPANSÃO DA UTILIZAÇÃO DOS *GADGETS* PARA FINS DIVERSOS E SUA RELAÇÃO COM A CONSUMERIZAÇÃO

Gadget é uma palavra inglesa que traduzindo significa "dispositivo" ou "aparelho". Consiste num dispositivo tecnológico que tem função específica e prática com grande utilidade no dia a dia. Amaral (2009) associa o termo *Gadget* a uma geringonça tecnológica. Esse dispositivo é conhecido pela inovação em tecnologia, sendo considerado um aparelho inteligente, incomum e eficiente.

Bem antes da revolução tecnológica, o homem fazia uso dos *Gadgets*, mesmo sem saber, como por exemplo, o relógio de pulso e a bússola. Nesta época, a pessoa que inventava era dotada de características um tanto especiais, o grau de inteligência era considerado acima da média, mesmo sem boa instrução. A invenção era desenvolvida de forma caseira, devido à inexistência de recursos, onde a pessoa que inventava era obrigada a deixar a escola a qual era dotada de um sistema fraco de ensino, para focar em suas pesquisas. Estes gênios da época, nem sempre tinha recurso para montar seu laboratório de pesquisa ou a sorte de ter sua pesquisa financiada por companhias interessadas em seus inventos.

A Revolução Tecnológica em conjunto com a Internet reformulou radicalmente os *gadgets*, mas mesmo assim, não perderam as características básicas das versões antigas; câmera fotográfica ainda hoje compete mercado com smartphones devido à existência de um público com preferências pessoais. Enquanto a Tecnologia oferece recursos à imaginação dos desenvolvedores, a Internet possibilita a comunicação com os inventores de todo o mundo proporcionando inclusive, a criação de inventos a partir de outros. Para Castells (2003) a Internet chegou para inovar os meios de comunicação por possibilitar o tráfego de informações entre os mais variados tipos de usuários, por tempo indeterminado e de modo global.

A tecnologia futura é apenas uma evolução do que já existe e que torna os *gadgets* cada vez mais impressionantes. Esses dispositivos da era moderna satisfazem as necessidades e desejos mais variados, onde a cada momento surge uma nova demanda exigindo o desenvolvimento de novos *gadgets*. É um ciclo sem fim que graças à Tecnologia hoje disponível, os desejos e necessidades do mercado são atendidos de forma surpreendente.

Devido à necessidade de se manter informado e adquirir conhecimento, o homem se torna cada dia mais dependente do uso de *Gadgets* (ou dispositivos eletrônicos), não somente na vida pessoal como também no trabalho.

Com o lançamento dos *smartphones* no mercado, não muito tempo atrás, alavancou-se uma revolução na tecnologia e na forma de compartilhamento e comunicação. A partir de então, outras plataformas começaram a surgir, seguindo a mesma tendência destes modelos de celulares que se conecta a internet em qualquer lugar, consumindo e compartilhando informações de maneira prática e simples. Do mesmo modo que os celulares inteligentes, surgiu as TVs inteligentes, ou SmartTVs, o mesmo aconteceu com DVD's, Blu-Rays e Home Theaters com função de conectividade *on line*.

A cada dia um novo *Gadget* é fabricado para atender a demanda do consumidor moderno caracterizado por saber escutar, interagir e compartilhar de maneira muito rica, suas experiências com produtos e serviços.

Se por um lado o consumidor busca tecnologia, praticidade e inovação, ele procura obter a mesma estrutura no ambiente de trabalho graças ao acelerado e atual avanço tecnológico. Diante deste fato, a organização interessada em mudar seu modelo de negócio vem se adaptando no mesmo ritmo, através do planejamento estratégico para obtenção de vantagem competitiva. De acordo com Stair e Reynolds (1999) "para se obter vantagem competitiva, uma empresa precisa ser rápida, ágil, flexível, inovadora, produtiva, econômica e orientada para o cliente." A empresa com visão estratégica busca incorporar novidades e desafios em sua cultura organizacional, mantendo sempre o foco na redução dos riscos com a Segurança da Informação, exposição financeira e caos no gerenciamento, para proporcionar o melhor resultado através do trabalho executado com satisfação do profissional.

Stair e Reynolds (1999) afirmam que para a organização permanecer ou se tornar competitiva, é necessário praticar a reengenharia em seus processos, tarefas e atividades.

> "A reengenharia, também chamada de redesenho dos processos, envolve a readequação dos processos empresariais, estruturas organizacionais, sistemas de informação e valores da organização, objetivando uma guinada nos resultados do negócio. A reengenharia pode reduzir o tempo de entrega de produtos, aumentar a qualidade do produto e do serviço, aumentar a satisfação do cliente e elevar o faturamento e a lucratividade." (STAIR E REYNOLDS, 1999:39)

Em paralelo com a reengenharia de processos, novos desafios são lançados à empresa ao lidar com o novo. Mudar a forma de trabalho das pessoas pode causar uma rígida resistência ou dificuldades em manter a mudança e alterações nos valores da organização e colaboradores.

Diante da crescente demanda, facilidade e interesse das pessoas em adquirir as últimas versões e lançamentos de *gadgets* no mercado do que as organizações em sua estrutura patrimonial, novos desafios surgem para o administrador que precisa controlar e responder à altura a essa crescente força conhecida como Consumerização.

A utilização de dispositivos móveis não é mais novidade, seja na vida pessoal ou em situações de trabalho. A mobilidade hoje ofertada no mercado torna-se a causa da empresa não conseguir controlar o uso dos equipamentos pessoais de seus colaboradores e permitir o contato entre as pessoas de forma ininterrupta e sem limites de distância. É fato que o número de profissionais, em qualquer setor organizacional, é muito grande e isso pode gerar muitas dúvidas e, até mesmo, certo desespero por parte da alta administração da empresa, que acaba se preocupando com a produtividade e com questões de segurança quando os dispositivos são conectados à rede corporativa. Com isso, o empresário deve estar disposto a entender e organizar este cenário, e não em combatê-lo.

A Consumerização nos negócios, também conhecida pela expressão BYOD (*Bring Your Own Device*), está crescendo de forma acelerada e com ela, a produtividade organizacional. Consiste numa tendência que está naturalmente se instalando na vida de empresas e profissionais.

De acordo com a redação da Cio (2011) a Consumerização consiste na inclusão de dispositivos móveis em uma organização, com o objetivo de aumentar a produtividade e diminuir os custos, deixando o funcionário livre para escolher e comprar o equipamento de sua preferência para executar suas atividades. Todavia, com esta permissão, os riscos relativos à segurança da empresa tendem a aumentar, dificultando a ação dos profissionais de TI. A

Consumerização está interligada de forma direta com a facilidade de uso, interfaces atraentes e funcionalidades variadas, sendo requisitos fundamentais para a atratividade de aquisição por parte dos funcionários.

É uma tendência que permite o colaborador utilizar em seu ambiente de trabalho seu dispositivo pessoal, proporcionando grandes vantagens para a empresa, como redução de gastos, por exemplo, e para os usuários, motivação e produtividade.

Em 2009, a Intel iniciou a prática do BYOD após o reconhecimento da potencialidade do método para promover a interação entre colaboradores e organização. Atualmente, o avanço tecnológico e a globalização presente no mercado brasileiro requerem dos profissionais, soluções para os negócios corporativos a qualquer momento e a qualquer hora, onde transações são negociadas e fechadas com fornecedores do outro lado do mundo viabilizadas graças à utilização dos dispositivos eletrônicos envoltos da tecnologia.

Em meados de 2011 ouviu-se o termo Consumerização no Brasil, advindo da cultura coorporativa internacional e que a partir de então, vem crescendo de forma acelerada, onde de acordo com que esta prática se espalha junto com a liberdade, agilidade e produtividade proporcionada ao usuário e à organização, traz também riscos dignos de atenção. Esses riscos que tanto empresa e colaboradores estão vulneráveis podem acarretar em perdas e riscos para o sucesso da aplicação da Consumerização nos negócios. O desafio então é conciliar esta tendência com a execução de atividades seguras, responsabilidade essa do setor de TI, proporcionando ao colaborador satisfação em exercer sua função, e segurança aos executivos, no que tange o tráfego dos arquivos e dados corporativos.

Para que o BYOD seja implementado no meio corporativo, então, é necessário se ter uma infraestrutura adequada para que seja oferecido o suporte necessário quando preciso: um grau elevado de maturidade, uma política de Segurança da Informação bem elaborada, um setor jurídico ativo em conjunto com um setor de Gestão de Pessoas preparado, estrutura de suporte adequada e uma equipe atuante de Tecnologia da Informação, pois, depois que esta tendência se torna prática, torna-se uma ferramenta de operação diária e controle contínuo.

2.2. A CONSUMERIZAÇÃO PELA ÓTICA DA SEGURANÇA DA INFORMAÇÃO

Observa-se que a segurança é um fato presente nos mais diversos cenários e uma questão preocupante tanto para as pessoas como para empresas, deixando de ser um simples complemento a uma necessidade.

A segurança dá cobertura a diversos setores da empresa, cada uma delas com seus próprios riscos, ameaças potenciais, controles aplicáveis e soluções de segurança que podem minimizar o nível de exposição ao qual a empresa está visível, com o objetivo de garantir segurança para a informação: seu mais importante patrimônio. De acordo com Foina (2009) a informação pode ser definida como:

> "(...) um dado (ou valor) associado a um conceito claro, não ambíguo e de conhecimento de todos os interessados, que seja acompanhado de uma referência para efeito de comparação e possa trazer vantagens competitivas para a organização. Normalmente a conceituação e as referências não acompanham o dado correspondente, mas deve-se garantir que todos os interessados naquela informação tenham os menos conceitos e referências sobre ela. Dados que não tenham utilidade, para uma pessoa ou para uma organização, não são informações e podem ser descartados." (FOINA, 2009:3)

Analisando a definição de Foina (2009) a informação é o conjunto de dados ordenados que, se emitida sob a forma e tempo adequados e com veracidade no conteúdo, melhora o conhecimento de quem recebe, e permite um melhor desenvolvimento de determinada atividade, ou a tomada de melhores decisões seja no âmbito operacional, tático ou estratégico. Logo, a informação deve ser clara e precisa, pois irá orientar as oportunidades e sinalizar as ameaças que as organizações estão sujeitas a se deparar pelo caminho, diminuindo as incertezas no decorrer do processo de tomada de decisão interferindo assim, positivamente na qualidade.

A informação propagada de forma segura, até algum tempo atrás antes da presença desta onda tecnológica, era interpretada como uma questão simples, pois os documentos em papéis podiam ser guardados de forma física em arquivos, mas, com o surgimento de tecnologias de informação e comunicação, a questão tornou-se um desafio, pois hoje a maioria dos computadores conectam-se à internet e a comunicação é feita através do envio e recebimento de dados digitais o que corresponde a um atrativo para usuários mal intencionados. Não bastando, existem também variadas situações de insegurança que podem afetar os sistemas de informação, como incêndios, alagamentos, problemas elétricos, poeira, fraudes, uso inadequado dos sistemas, engenharia social, guerras, seqüestros, etc.

Para Chiavenato (2003) “a tecnologia passa a constituir a principal ferramenta a serviço do homem e não mais a variável independente e dominadora que impunha condições tanto à estrutura como ao comportamento das organizações, como ocorria nas duas eras industriais anteriores”. Para o autor, a tecnologia antes vista como um acessório dominador, hoje é analisado como um fator estratégico organizacional devido ser hoje a responsável por armazenar, recuperar, processar, divulgar e propagar a informação a qual deve ser implementada com a segurança necessária ao seu tráfego.

Contudo, toda tecnologia tem suas falhas, sendo então necessária a descoberta dos pontos vulneráveis e posteriormente, analisar os riscos e os impactos para então, rapidamente, tomar providências para que a Segurança da Informação seja eficaz. Na prática muitas organizações não dão o devido valor a esta questão e na maioria das vezes, o custo é bem elevado. Com isso, a melhor alternativa é reduzir ao máximo quaisquer riscos às informações, seguindo um trajeto na direção de se manter a integridade e a disponibilidade dos sistemas de informação.

Para Fontes (2006) a “Segurança da informação é o conjunto de orientações, normas, procedimento, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada”. A Segurança da Informação surgiu para minimizar os riscos causados pela utilização dos recursos de informação, para garantir que a informação seja acessível apenas às pessoas autorizadas, para proteger a exatidão e estado completo da informação e dos métodos de processamento bem como garantir que as pessoas autorizadas tenham acesso às informações, e aos bens associados, quando requeridos.

A norma ABNT NBR ISO/IEC 27002:2005, a qual foi substituída pela ABNT NBR ISO/IEC 27002:2013, estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de Segurança da Informação em uma organização. Os objetivos definidos nela descrevem diretrizes gerais sobre os resultados geralmente aceitos para a gestão de Segurança da Informação. Esta norma descreve que a Segurança da Informação é a proteção da informação de diversos tipos de ameaças que garantam a continuidade do negócio, diminuindo os riscos e aumentando o retorno sobre investimentos e oportunidades de negócio.

A implantação de um eficaz sistema de segurança de informação dentro de uma empresa requer dos integrantes dos níveis tático e estratégico atenção especial no que diz respeito à análise dos riscos, à definição da Política de Segurança e por fim ao desenvolvimento de um plano de contingência. A análise dos riscos basicamente tem objetivo de identificar os pontos fracos em que a informação está exposta, identificando desta maneira quais os pontos que necessitam de maior empenho em proteção. A Política de Segurança da informação consiste na formalização de ações a serem tomadas de forma a garantir a segurança e disponibilidade dos mesmos, sendo de suma importância para o uso seguro da informação. Os planos de contingência, por sua vez, também possuem objetivo fundamental, pois descreve a ação a ser tomada em caso de problemas com as informações.

Para obter a Segurança da Informação em um nível satisfatório se faz necessário um conjunto de controles e mecanismos de segurança adequados que a organização deve aderir, com intuito de garantir que os objetivos do seu negócio e de segurança sejam alcançados.

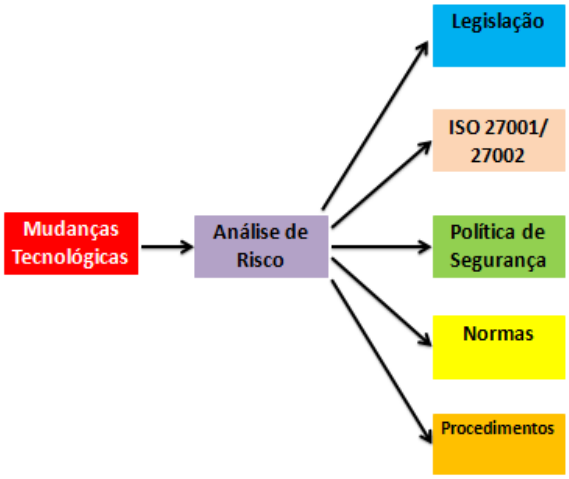

Figura 1: Visão geral da Segurança da Informação.

A Figura 1 mostra que mudanças tecnológicas estão diariamente presentes na organização as quais proporcionam o surgimento de novos riscos e vulnerabilidades ou ocasionam o aumento dos já existentes, necessitando o acompanhamento de análise dos riscos de forma constante permitindo assim o maior controle e a melhor maneira de tratá-los. Ao mesmo tempo, se faz necessário o conhecimento da legislação que envolve toda a estrutura empresarial e o levantamento dos requisitos necessários de segurança para atendê-la, onde a partir destes fatores legais, identificam-se os controles necessários e aqueles evidenciados pela análise de riscos, com a utilização das normas de segurança. Através da identificação dos controles, é necessário desenvolver as políticas, normas e procedimentos para a implementação dos mesmos.

A Segurança da Informação aliada à iniciativa de preservação da Confidencialidade, Integridade e Disponibilidade com a aplicação de normas em toda sua estrutura, faz com que os gestores tenham maior controle sobre os processos organizacionais tornando-se cada vez mais eficaz e paralelo aos objetivos da empresa, proporcionando o desejado sucesso nas negociações no atual mercado dinâmico, globalizado e competitivo.

Observa-se que a análise dos sistemas de segurança de informações vem sendo debatidas entre os gestores devido à globalização, que traz consigo inúmeras vantagens e facilidades na comunicação e articulações comerciais nas empresas, redução de tempo para solucionar os problemas, entre outras coisas. A partir disso, com a tendência competitiva do mercado atual em utilizar estratégias tecnológicas para se sobressair dos concorrentes, a

tecnologia da informação vem evoluindo no mesmo ritmo. Além do mais, a concorrência utiliza as falhas nos sistemas de informação para fazer espionagem ou prejudicar os negócios da empresa, sendo necessário mais do que nunca, a utilização de sistemas de segurança cada vez mais evoluídos. Como dito antes, não existe uma segurança plena, sem risco ou danos para o usuário ou empresa, mas espera-se que sua utilização seja eficaz.

Hoje as organizações ou mesmo os detentores de informações importantes, precisam estar atentos para qualquer abertura que possa deixar o sistema de Segurança da Informação vulnerável. Assim sendo, do mesmo modo que uma empresa precisa oferecer qualidade nos serviços, precisam também se adequar as necessidades de segurança, para que, no futuro, não venha sofrer com os próprios erros, no caso, não defender tecnologicamente o seu patrimônio.

Segundo Sambucci (2013) alguns riscos a segurança da informação são gerados com a prática da Consumerização pelas organizações, como a divulgação acidental de informações da empresa; exclusão dos dados de forma acidental; roubo de dados de forma intencional e acesso não autorizado.

A divulgação acidental de informações da empresa ocorre quando a informação é copiada sem criptografia pelo usuário e o mesmo perde ou tem seu aparelho furtado, colocando em risco os dados sigilosos da empresa.

A exclusão dos dados de forma acidental é ocasionada quando as informações pessoais de um servidor são acessadas a partir de um dispositivo móvel que contenha aplicativos deficientes em segurança (como aplicativos baixados gratuitamente na internet) abrindo as portas para a entrada de *malwares*. O usuário pode também receber vírus através do acesso à e-mails em seu dispositivo e espalhar aos colegas de trabalho “contaminando” a rede da empresa.

O roubo de dados de forma intencional acontece quando o usuário malicioso salva dados confidenciais em seu dispositivo através da rede corporativa.

O acesso não autorizado ocorre quando o usuário invade o servidor da empresa e rouba dados confidenciais.

Ainda de acordo com Sambucci (2013) algumas recomendações são enfatizadas como forma de minimizar os riscos à Segurança da Informação, promover a criação de um ambiente colaborativo e proporcionar uma melhor contribuição para o alcance dos objetivos da empresa com a utilização dos *Gadgets* dentro da empresa. Essas recomendações compreendem o desenvolvimento de um inventário de dispositivos; a avaliação de como os dispositivos estão sendo usados; a aquisição de software de gerenciamento de dispositivos móveis; a criação de uma política de acesso ao dispositivo, de proteção e de uma política de Consumerização; a elaboração de uma lista dos aplicativos confiáveis; o estabelecimento de uma listagem de aplicativos de uso obrigatório; a criação de uma campanha de divulgação da nova política; a garantia de serviços de backup; a definição de regras e procedimentos para auditorias; o estabelecimento dos sistemas operacionais permitidos bem como do limite entre o pessoal e profissional.

A organização deve desenvolver um inventário e manter o registro de todos os dispositivos móveis usados para acessar a rede da empresa. Este inventário deve conter, entre outras informações: Nome do funcionário e função; Tipo de dispositivo (Smartphone, Tablet, Notebook etc); Modelo e fabricante; Sistema operacional; Número de série; Relação dos aplicativos usados que tenham acesso à rede. Em caso de desligamento do funcionário, deve ser comunicado para que seja removido e-mails, acesso à rede de dados, entre outras informações.

O departamento de TI deve criar uma política de acesso, onde cada dispositivo possuirá a autorização devida aos recursos selecionados.

Deve ser também elaborada uma política de proteção do dispositivo, como criptografia e senha de acesso. A política de proteção deve incluir outros requisitos de segurança, como por exemplo: Nunca deixar o aparelho sem vigilância; Informar imediatamente sobre a perda ou roubo do *gadget* ao departamento de TI; Informar ao departamento de TI antes da venda ou repasse do dispositivo para terceiros; Não emprestar o aparelho.

A criação de uma política de Consumerização (BYOD) irá definir como os dispositivos móveis são usados no trabalho. O uso correto dos dispositivos é vital para a segurança da rede e seus dados. A política se relacionaria, por exemplo, aos deveres dos funcionários quanto ao uso responsável de: *E-mail* corporativo acessado em dispositivos móveis; Aplicativos usados enquanto o dispositivo está conectado à rede da empresa; Conexões simultâneas para outras redes (por exemplo, 3G) ou outros dispositivos (por exemplo, *Bluetooth*) enquanto o gadget está conectado à rede corporativa; Dados pessoais compartilhados através de *e-mails* enviados ou *downloads* realizados enquanto o dispositivo está conectado à rede da empresa.

A criação de uma campanha de divulgação da nova política irá conscientizar os colaboradores, pois eles podem não conhecer ou nunca ter trabalho em um ambiente BYOD.

A necessidade da definição de regras e procedimentos para auditorias é devida para verificação dos dispositivos, ou seja, analisar se eles estão sendo utilizados conforme as normas estabelecidas na política BYOD. O departamento de TI deve trabalhar em conjunto com o departamento Jurídico e de Gestão de Pessoas para criar regras que permitam procedimentos de auditoria eficazes.

A elaboração de uma lista dos sistemas operacionais permitidos no ambiente BYOD é de suma importância. Hoje, existem dois principais sistemas operacionais móveis, o Android e iOS, o que torna mais fácil para a indústria de segurança desenvolver aplicativos de proteção. Isto, portanto, não significa que seja mais fácil para os departamentos de TI, uma vez que seu trabalho é proteger todos os dispositivos usados pelos funcionários, não importando o sistema operacional em uso. O departamento de TI tem uma escolha: ou todos são aceitos e políticas e procedimentos são concebidos para cada sistema operacional diferente ou apenas alguns sistemas selecionados terão permissão para se conectar a rede. A escolha depende principalmente dos recursos disponíveis pela organização, embora seja seguro assumir que a maioria das empresas poderá optar pela não autorização de sistemas operacionais desconhecidos.

Estabelecer o limite entre o pessoal e profissional é um desafio que a organização precisa resolver. O funcionário BYOD pode trabalhar sem hora nem local fixos podendo gerar frustração em longo prazo e até trabalho extra não remunerado.

Estas recomendações são um alerta para o gestor que pretende implementar ou que já pratica a Consumerização e precisa aperfeiçoar. A Consumerização já faz parte do processo atual de transformação da TI, e será inevitável conviver com ela a partir de agora. Além destas recomendações, o importante para os gestores é entender o que é a Consumerização, como ela pode agregar valor ao seu negócio, e como sua empresa deve preparar-se e antecipar-se a ela.

Após uma longa lista de ameaças e recomendações, adotar o modelo BYOD pode parecer uma má idéia, porém, ainda de acordo com Sambucci (2013), utilizar os Gadgets no trabalho proporciona grandes vantagens tanto para empresa quanto para o funcionário, como: maior produtividade; redução de custos; versatilidade de conexão; satisfação e envolvimento do funcionário e mobilidade.

O aumento da produtividade é conseqüência da facilidade que o funcionário tem de trabalhar fora do ambiente organizacional, proporcionando satisfação profissional.

A redução de custos com equipamentos de informática e/ou telecomunicações é significativa devido à empresa utilizar o dispositivo tecnológico adquirido por seu funcionário.

A versatilidade de conexão é conseguida graças à tecnologia disponível atualmente, onde todo e qualquer dispositivo móvel podem ser conectados através da rede sem fio WI FI ou pela rede 3G, por exemplo, disponibilizada pela operadora telefônica. Logo, na indisponibilidade da rede corporativa, o funcionário pode alternar a conexão para a 3G, a qual deve inclusive, ser regulamentada por uma política de utilização.

A satisfação e envolvimento do funcionário é alcançada devido à empresa permitir o uso de seu dispositivo pessoal para fins profissionais, o qual irá trabalhar com maior satisfação e ao mesmo tempo beneficiará a empresa através de uma significativa redução de custos e de um aumento considerável na produção.

A mobilidade irá permitir que o funcionário trabalhe e tenha acesso a seus documentos de qualquer lugar, a qualquer hora e, o melhor, através de seu próprio dispositivo.

Diante das vantagens proporcionadas ao negócio no modelo BYOD, é necessário parar de tratar a questão como se fosse um problema de policiamento, e abordá-la como gestão de risco. As vantagens são muitas, mas os riscos devem ser levados em consideração para a eficácia dos resultados. Portanto, tão importante quanto sair na frente e usufruir dos ganhos de competitividade que BYOD traz, é planejar como se dará sua implantação na empresa. Os novos patamares de mobilidade, agilidade e produtividade devem ser sustentados por infraestrutura e políticas sólidas.

3. METODOLOGIA

A base deste trabalho foi obtida através de entrevistas realizadas com Gestores de Recursos Humanos e de Tecnologia da Informação de três empresas distintas, localizadas na cidade de Volta Redonda. O questionário foi formulado como forma de identificar se os profissionais conhecem os termos Consumerização ou BYOD, se a empresa em que atuam autoriza a Consumerização em seus negócios e se adotam alguma Política de Segurança da Informação como forma de minimizar os riscos da referida prática.

Foi realizada uma pesquisa qualitativa de caráter exploratório estimulando os entrevistados a pensar e falar livremente sobre o tema, o questionário também possuía questões que foram tratadas como quantitativas. Através da pesquisa, foi identificada a visão do gestor de TI e RH sobre a aplicabilidade da Consumerização em uma empresa no Brasil e o que o gestor de RH exclusivamente, pensa sobre o grau de preparo da CLT diante de casos em que funcionários possam exigir na justiça o pagamento de horas extras por trabalharem fora de seu horário de expediente.

4. RESULTADOS

A questão número 1 da pesquisa teve como objetivo identificar se os gestores conhecem os termos Consumerização de TI ou a sigla BYOD aplicada em uma empresa.

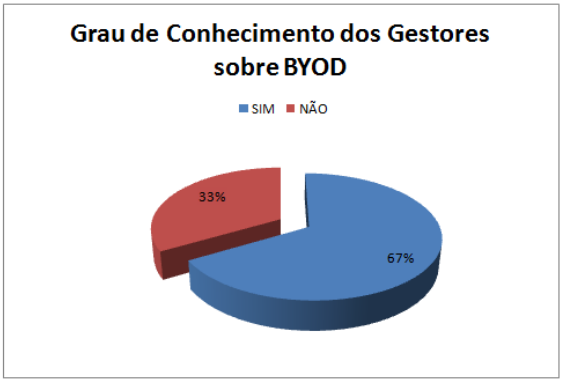

Gráfico 1: Grau de conhecimento dos gestores das empresas sobre o BYOD.

Através da questão 2 foi analisado se o gestor já leu sobre o assunto ou conhece alguma organização que pratica a Consumerização nos Negócios.

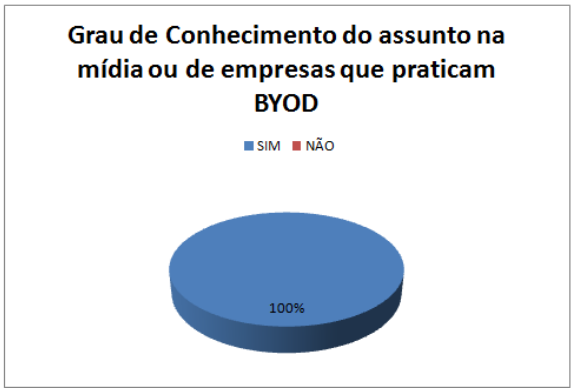

Gráfico 2: Conhece ou já leu sobre alguma empresa que pratica o BYOD?

Em caso positivo na questão 1, foi analisado através da questão 3 se a empresa em que os profissionais atuam praticam ou autorizam a Consumerização de TI com seus funcionários.

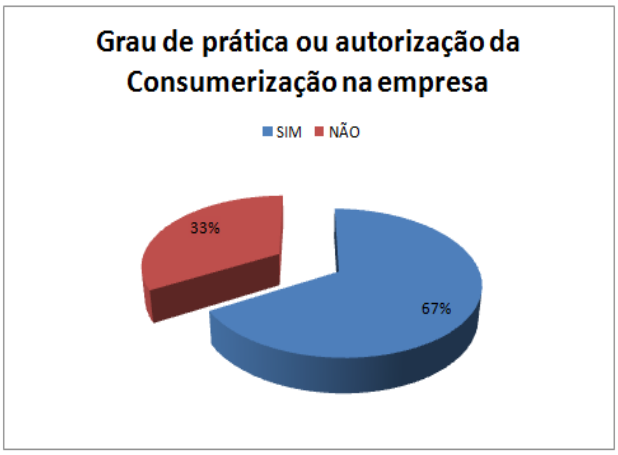

Gráfico 3: A sua empresa autoriza a prática de BYOD?

Através da questão 4, foi questionado aos gestores se a empresa em que atuam adota uma Política de Segurança da informação formal como instrumento para minimizar os riscos à Segurança da Informação pelos funcionários da empresa.

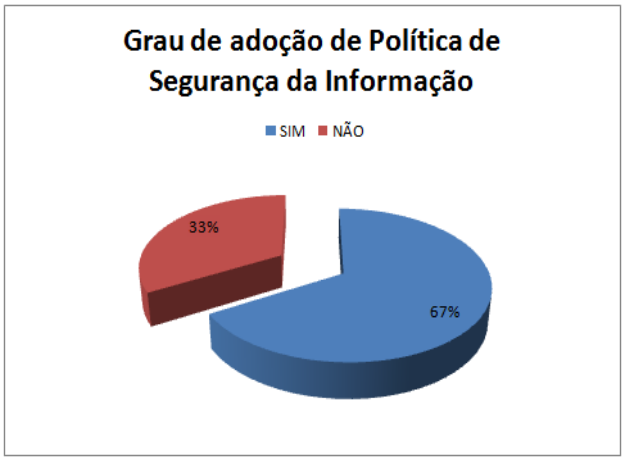

Gráfico 4: A sua empresa tem uma política de segurança da informação formalizada?

A questão 5, foi direcionada exclusivamente aos gestores de RH, onde foi analisada a opinião dos profissionais sobre o grau de abrangência da CLT diante de casos em que os funcionários possam exigir na justiça o pagamento de horas extras por trabalharem fora de seu horário de expediente. As respostas obtidas foram: A CLT não está preparada para esta filosofia de TI; Acreditam que deverá ocorrer inclusão de emendas na CLT o mais rápido possível; A metodologia é aplicável somente em empresas com muitos funcionários; As empresas não estão preparadas para essa prática no tocante à Segurança da Informação; As empresas devem investir em treinamentos aos funcionários desta prática.

A questão 5, direcionada exclusivamente aos gestores de TI, questionou a opinião dos profissionais sobre a aplicabilidade da Consumerização em uma empresa no Brasil, ou seja, o que cada um julgou como ponto positivo e/ou negativo diante da aceitação desta nova modalidade de negócio. Obtiveram-se as seguintes respostas como pontos positivos: o usuário pode escolher qual dispositivo usar, o que mais lhe agrada; ocorre aumento da produtividade, além da redução de custos na compra de equipamentos; mobilidade de trabalho; aumento da dinâmica no exercício das atividades profissionais. Como pontos negativos foram julgados: existência de risco à segurança dos dados corporativos causando indecisão na aplicabilidade da Consumerização nas empresas; dificuldade de visibilidade e controle do tráfego de dados fora do ambiente corporativo; carência no mercado de sistemas de segurança de informação confiáveis; inexistência de legislação pertinente ao assunto; melhor adaptação desta prática às empresas de grande porte.

A questão 6, direcionada aos gestores de RH, questionou a opinião dos profissionais sobre a aplicabilidade da Consumerização em uma empresa no Brasil, ou seja, o que cada um julgou como ponto positivo e/ou negativo diante da aceitação desta nova modalidade de negócio. Como pontos positivos, foram obtidos as seguintes respostas: redução dos custos com aquisição de equipamentos tecnológicos; mobilidade de trabalho; interação da vida pessoal e profissional; eficácia nos resultados devido o dinamismo na resolução de problemas e decisões. Como pontos negativos, foram considerados: falhas na Política de Segurança; vulnerabilidade das informações e cobrança de horas extras pelos funcionários na justiça; limite entre o pessoal e o profissional indefinido.

Na análise quantitativa dos dados da pesquisa observa-se que 67% dos entrevistados afirmam que além de conhecer a prática da Consumerização acreditam que a empresa que trabalham poderia autorizar tal prática no negócio.

Um ponto importante a destacar é que quando unimos as questões autorizar a prática de Consumerização no negócio e ao mesmo tempo, exigir a adoção de Política de Segurança de Informação, obtemos também um percentual de 67% o que demonstrou o ótimo grau de maturidade em relação a essa prática na visão dos gestores, exigindo um alinhamento estratégico entre RH e TI, além de construírem em conjunto, políticas e metodologias que irão minimizar os riscos à Segurança da Informação da empresa com essa prática.

Foram detectados pontos positivos e pontos negativos para auxiliar a adoção deste método nas empresas, mas como uma análise mais apurada definiu-se que para ser vantajoso, por exemplo, na produtividade dos funcionários, a adoção da Consumerização nos negócios deve necessariamente: exigir que os Sindicatos de Classe busquem junto aos órgãos executivos do Ministério do Trabalho criem parágrafo ou artigo específico na CLT para regular essa prática pelos funcionários; e as empresas devem investir em controles tecnológicos e humanos para minimizar os riscos associados à Segurança da Informação, bem como, escrever Políticas de Segurança eficazes e que tratem o tema com o grau de importância que ele exige.

5. CONCLUSÃO

Consumerização ou BYOD é a tendência que está sendo impulsionada com o uso de tecnologias simples, de fácil acesso e abrangência, através do qual as empresas adotantes deste modelo autorizam os colaboradores a trabalharem em qualquer hora e em qualquer lugar com dispositivos pessoais conectados à rede e aos Sistemas de Informação corporativos. O presente trabalho teve como objetivo analisar até que ponto é vantajoso para a empresa adotar a Consumerização nos negócios, ou seja, autorizar seu funcionário a utilizar seu dispositivo pessoal dentro da organização.

Quando a empresa autoriza o funcionário a fazer uso do próprio dispositivo é importante e indispensável a elaboração de uma boa Política de Segurança, visto que a mobilidade do aparelho ao mesmo tempo que é vantajoso para a organização e o funcionário, se torna perigoso com a vulnerabilidade de informações confidenciais da empresa.

Na pesquisa, analisaram-se três empresas distintas, localizadas na cidade de Volta Redonda, onde foi questionado aos gestores de RH e TI se eles conhecem os termos Consumerização ou BYOD. Identificou-se que esses profissionais conhecem ou já ouviram falar em Consumerização, porém alguns não conhecem a prática nas suas respectivas empresas. Mostrou-se também a grande preocupação dos gestores com a não abrangência da CLT sobre o tema, sobre a vulnerabilidade das informações e as falhas na Política de Segurança corporativa que necessita ser atualizada sobre o tema. Observa-se também, que os gestores têm uma base da utilização dos *gadgets* nas empresas e entendem seu valor como uma possibilidade no trabalho e se preocupam com os riscos que correm. A maioria dos gestores não adota uma Política de Segurança como instrumento para minimizar os riscos e não seguem as normas da ABNT ISO 27001 e 27002.

A hipótese da pesquisa tinha como objetivo analisar os riscos à Segurança da Informação com essa prática, e com isso, conclui-se que as empresas obtém vantagem competitiva por estarem atualizadas em relação à concorrência e otimização de tempo, recursos e redução de gastos e se a mobilidade for permitida ao profissional, os colaboradores se tornarão motivados em exercer sua função com conforto e praticidade, cujo desenvolvimento das atividades pelo colaborador torna-se mais produtivo e prazeroso.

Após a pesquisa, viu-se que se a empresa adotar uma boa Política de Segurança fizer uso das normas, criar uma política de Consumerização, criar uma campanha de divulgação, definir regras estabelecendo limites entre o uso pessoal e profissional torna-se vantajoso para a empresa adotar a Consumerização nos negócios visto que o funcionário trabalhará motivado, terá mais produtividade, redução de custos e mobilidade, agilizando assim a forma de trabalho.

Como sugestão para futuros estudos sobre o tema, poderia ser expandida a pesquisa de opinião também para os funcionários de escritório, pois com isso, teria-se uma análise da importância do tema com a visão dos gestores e também dos demais funcionários que efetivamente usarão tal tecnologia e conceito no dia a dia de seus trabalhos, criando-se assim, um estudo científico completo para que outros profissionais de gestão possam decidir com mais facilidade sobre autorizar ou não esta política moderna de trabalho de escritório.

6. REFERÊNCIAS

A evolução dos gadgets domésticos. Dez, 2013. Disponível em:

http://www.nerddisse.com.br/novidade/a-evolucao-dos-gadgets-domesticos/. Acesso em: 22 mar. 2014

ALVES, G. A. Segurança da Informação. Uma visão inovadora de gestão**.** Rio de Janeiro: Ciência Moderna, 2006.

ALMEIDA, A. L. P. de, MAZZA, A. *Vade Mecum* Trabalhista**.** 5. ed. rev. Ampl. São Paulo: Rideel, 2011.

AMARAL, F. E. O que é Gadget? E Widget, é a mesma coisa? Abril, 2009. Disponível em: http://www.tecmundo.com.br/1959-o-que-e-gadget-e-widget-e-a-mesma-coisa-.htm. Acesso em: 12 abr. 2014.

Art. 1016 do Código Civil – Lei 10406/02. Disponível em:

http://presrepublica.jusbrasil.com.br/legislacao/91577/codigo-civil-lei-10406-02#art-1016. Acesso em: 13 abr. 2014

ASCARI, J. A. B. BYOD – Você sabe o que é isso? Jan. 2014. Disponível em: http://coaliza.org.br/blog/BYOD-voce-sabe-o-que-e-isso-2/- Acesso em: 19 fev. 2014.

BRADLEY, J. et al. BYOD: uma perspectiva global aproveitando a inovação liderada pelo funcionário. Disponível em:

http://www.cisco.com/web/about/ac79/docs/re/BYOD/BYOD_Horizons_Global_PTBR.pdf. Acesso em: 19 fev. 2014.

CASTELLS, M. A Galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003.

CIO. Consumerização: aliada ou inimiga da equipe de TI? Out, 2011**.** Disponível em: http://computerworld.com.br/tecnologia/2011/10/05/consumerizacao-aliada-ou-inimiga-da-equipe-de-ti/. Acesso em: 23 fev. 2014.

CHIAVENATO, I. Introdução a teoria geral da administração: uma visão abrangente da moderna administração das organizações. 7ª ed. rev. e atual. Rio de Janeiro: Elsevier, 2003.

COELHO, F. E. S., ARAUJO, L. G. S. Gestão da Segurança da Informação. Rio de Janeiro: Escola Superior de Redes, 2013.

FOINA, P. R. Tecnologia de Informação: Planejamento e Gestão. 2. Ed. São Paulo: Atlas, 2009.

FONTES, E. Segurança da informação: o usuário faz a diferença. São Paulo: Saraiva, 2006.

Gadgets. Disponível em:

http://canaltech.com.br/tag/Gadgets/Analises/5.html#ixzz2wWqXMPfG. Acesso em: 20 mar. 2014.

Gadget. Disponível em: http://pt.wikipedia.org/wiki/Gadget. Acesso em: 20 mar. 2014.

GOLDEN, B. O que a Consumerização realmente significa para as empresas? Ago, 2011. Disponível em: http://computerworld.com.br/tecnologia/2011/08/12/o-que-a-consumerizacao-realmente-significa-para-as-empresas/. Acesso em: 23 fev. 2014.

INGRAHAM, N. Google purchases Nest for $3.2 billion. Jan, 2014. Disponível em: http://www.theverge.com/2014/1/13/5305282/google-purchases-nest-for-3-2-billion. Acesso em: 22 mar. 2014

LUCA, C. de. BYOD ganha impulso no Brasil a partir de 2014. Ago, 2013. Disponível em: http://computerworld.com.br/negocios/2013/08/14/BYOD-ganha-impulso-no-brasil-a-partir-de-2014-diz-pesquisa/. Acesso em: 04 mar. 2014.

O que é a norma ISO 27001? Disponível em: http://www.ISO27001.pt/. Acesso em: 23 fev. 2014.

Os gadgets do futuro. Disponível em: http://revistaalfa.abril.com.br/tecnologia/gadgets/os-gadgets-do-futuro/. Acesso em: 20 mar. 2014.

Produtividade é o maior benefício do BYOD, aponta pesquisa. Disponível em: http://www.fenainfo.org.br/info_ler.php?id=42522. Acesso em: 20 mar. 2014.

REZENDE, D. A., ABREU, A. F. de. Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais. O papel estratégico da Informação e dos Sistemas de Informação nas Empresas**.** 4. ed. rev. ampl. São Paulo: Atlas, 2006.

SAMBUCCI, L. Emerging threats for the healthcare industry: the BYOD revolution**.** Deepsecurity, 2013.

STAIR, R. M., REYNOLDS, G. W. Principios de Sistema da Informação. Uma abordagem gerencial**.** 4. ed. rev. ampl. São Paulo: LTC, 1999.

TALARICO, S. BYOD e Consumerização: o que são e como utilizar? Ago, 2013.

Disponível em: http://www.businessreviewbrasil.com.br/technology/gadget/BYOD-e-consumerizacao-o-que-sao-e-como-utilizar. Acesso em: 19 fev. 2014