- *Revista EDUCAmazônia - Educação Sociedade e Meio Ambiente, Humaitá,* **LAPESAM/GISREA/UFAM/CNPq/EDUA –**
ISSN 1983-3423 – IMPRESSA – ISSN 2318 – 8766 – CDROOM – ISSN 2358-1468 - DIGITAL ON LINE

Vol XVI, Núm 2, jul-dez, 2023, pág. 497-510

BRING YOUR OWN DEVICE (BYOD): QUAIS AS VANTAGENS E DESVANTAGENS QUE PODEM TER NAS ORGANIZAÇÕES NO CONTEXTO DE SEGURANÇA DA INFORMAÇÃO

BRING YOUR OWN DEVICE (BYOD): WHAT ADVANTAGES AND DISADVANTAGES ORGANIZATIONS MAY HAVE IN THE CONTEXT OF INFORMATION SECURITY

Ideir Coto[1]
Pedro Vinícius Rodrigues Dias[2]

RESUMO

Com a consumerização de TICS– Tecnologias da Informação e da Comunicação está forçando as organizações a se adaptarem a novas maneiras de atuarem no mercado, diante de um ambiente mercadológico cada vez mais competitivo. No sentido de auxiliar as organizações a conquistarem seus objetivos mercadológicos, há uma tendência para consumir computadores que está revolucionando o funcionamento das organizações. Essa tendência permite ao colaborador a atuar dentro da organização por meio de seus dispositivos pessoais, a qual é conhecida por BYOD, termo inglês que significa *Bring Your Own Device* – Traga Seu Próprio Dispositivo). Esse conceito tem um impacto positivo nos resultados das organizações – principalmente, no que diz respeito ao clima organizacional –, mas também oferece determinados riscos para a segurança da informação destas organizações. Com base nesse contexto, a presente pesquisa analisou os principais aspectos relacionados a segurança em redes de computadores com ênfase no conceito BYOD, destacando o seguinte questionamento: quais são as principais vantagens e desvantagens para a segurança da informação das organizações que adotam o conceito de BYOD? Em relação ao objetivo deste estudo, foram analisadas as principais características referentes à segurança da informação nas organizações, com ênfase no conceito BYOD.

Palavras-Chave: Redes sem fio, BYOD, mobilidade, dispositivos**,** Clima Organizacional. Tecnologias da Informação e da Comunicação. Ambiente Mercadológico. Segurança da Informação.

ABSTRACT

With the consumerization of TICS – Information and Communication Technologies is forcing organizations to adapt to new ways of operating in the market, in the face of an increasingly competitive market environment. In order to help organizations achieve their marketing goals, there is a tendency to consume computers that is revolutionizing the way organizations work. This trend allows the employee to work within the organization through their personal devices, which is known as BYOD (Bring Your Own Device). This concept has a positive impact on the results of organizations – mainly, with regard to the organizational climate –, but it also poses certain risks to the information security of these organizations. Based on this context, this research analyzed the main aspects related to security in computer networks with emphasis on the BYOD concept, highlighting the following question: what are the main advantages and disadvantages for information security of organizations that adopt the BYOD concept ? Regarding the objective of this study, the main characteristics related to information security in organizations were analyzed, with emphasis on the BYOD concept.

[1] Mestrado em Administração pela Universidade Paulista(UNIP). Professor do Instituto Federal de Rondônia IFRO – *campus* Guajará-Mirim. E-mail: ideir.coto@ifro.edu.br

[2] Analista de Sistemas pela São Lucas Ji-Paraná-RO e Pós Graduado em Ciência de Dados pela UNIASSELVI. Técnico em Tecnologia da Informação na Universidade Federal do Amazonas (UFAM). E-mail: pedrovinny2@gmail.com

Keywords: Wireless networks, BYOD, mobility, devices, Organizational Climate. Information and Communication Technologies. Marketing Environment. Information security.

INTRODUÇÃO

As redes sem fio (também conhecido pelo termo em inglês wireless network) são um serviço essencial para organizações em todos os segmentos de mercado. Muitas indústrias não podem mais imaginar suas atividades diárias sem conexão sem fio, forçando as instituições a investir cada vez mais em um serviço móvel completo e eficiente (KUROSE, 2010).

Inicialmente, as empresas planejavam suas redes sem fio para usar seus dispositivos exclusivamente, normalmente estações de trabalho totalmente configuradas e gerenciadas internamente, e de acordo com governança em TI (Tecnologia da informação) que segundo Lyra, Mauricio Rocha (2015) tem o controle total sobre o que está instalado, o acesso autorizado e restrições. O usuário do dispositivo não pode alterar uma regra deste ambiente, mas com o avanço da tecnologia móvel e uma redução significativa no custo de *tablets* e smartphones e *laptops*, o uso desses dispositivos cresceu fortemente nas redes de organizações (KUROSE, 2010).

Uma nova tendência em tecnologia para uso pessoal está sendo adotada por organizações, revolucionando o desempenho diário dos funcionários. Esta prática é conhecida pela abreviatura BYOD (*Bring Your Own* Device) - Traga seu dispositivo - ou o termo consumerização, de acordo com Gartner (2013), a consumerização é caracterizada pelo impacto oriundo das tecnologias trazidas pelos colaboradores ao ambiente empresarial. Em outras palavras, é o modelo em que o colaborador traz seus equipamentos pessoais de trabalho, como smartphones, *tablets* ou *laptops* e trabalha com esses aparelhos (BEAL, 2005).

Quando uma empresa consome e seus funcionários trabalham com seu próprio dispositivo, a empresa recebe tempo, recursos e gastos de TI reduzidos. Quando a mobilidade é permitida para o praticante, o colaborador é motivado a desempenhar sua função com facilidade e conforto, cujo desenvolvimento se torna mais produtivo e agradável em seu trabalho (BEAL, 2005).

O funcionário que adota o termo BYOD se sente motivado e adquire um dispositivo eletrônico que ofereça maior afinidade e melhor execução de suas atividades. Como resultado, a empresa aumenta suas taxas de produtividade e reduz seu investimento em compras ou atualizações. Nível de dispositivos para seus funcionários. Ao mesmo tempo, a BYOD está forçando a organização a desenvolver e implementar uma estratégia excelente que deve

incorporar uma política de segurança da informação bem desenvolvida que também inclua problemas de trabalho (BEAL, 2005).

BYOD: Conceitos, Vantagens e Desvantagens em relação à Segurança da Informação nas Organizações

Cada vez mais, os usuários possuem seus próprios dispositivos que podem realizar todas as atividades anteriormente realizadas pelas equipes do instituto. O uso de computadores de mesa diminuiu nos últimos anos e, na direção oposta, o uso de dispositivos móveis está aumentando, sendo este fato referido como consumação de computadores. BYOD - ou a consumerização - é a tendência das tecnologias desenvolvidas que visam penetrar no mercado consumidor no mundo dos negócios.

O consumo foi impulsionado pelo forte crescimento no mercado consumidor, onde os fabricantes de eletrônicos foram forçados a produzir aparelhos e disponibilizá-los em comparação com eletrodomésticos de menor valor. O BYOD permite o desenvolvimento de dispositivos com plataformas de aplicativos mais inteligentes e serviços personalizados, tais como computação em nuvem e redes sociais (DODT, 2013; GARANHANI, 2013).

Claro, em comparação com as afirmações dos autores citadas acima, seria esperado que os usuários móveis (celulares, *tablets*, *laptops*) não usassem mais esses dispositivos tão profundamente quanto objetivos pessoais, usá-los para fins profissionais e acadêmicos, conectar-se com empresas e às faculdades onde desempenham seus deveres. Essa tendência é chamada BYOD (Traga seu dispositivo).

O fenômeno causado pelo consumo de dispositivos móveis, onde as pessoas se voltaram para o uso de seus dispositivos pessoais para fins comerciais e pessoais, tornou-se conhecido como BYOD (*Bring Your Own Device*). Para o grande número de empresas, principalmente na Ásia e na América Latina, BYOD é visto com bons olhos porque aumenta a produtividade e a satisfação dos funcionários e o custo de aquisição de equipamentos (BRADLEY et al., 2012).

O consumo corporativo, também conhecido como BYOD (*Bring Your Own Device*), está crescendo rapidamente, e com ele, a produtividade da organização. Esta é uma tendência que pode ser encontrada na vida de empresas e profissionais. O consumo é a inclusão de dispositivos móveis em uma organização para aumentar a produtividade e reduzir custos para que o colaborador possa escolher e comprar livremente o equipamento de sua escolha para realizar suas atividades. No entanto, esta aprovação aumenta os riscos associados à segurança do

negócio, prejudicando as ações dos profissionais de TI. A consumerização está diretamente relacionada à usabilidade, interfaces atraentes e várias funcionalidades, que é um pré-requisito para a atratividade da aquisição de funcionários (COMPUTERWORLD, 2011).

É uma tendência que permite que os funcionários usem seu dispositivo pessoal em seu ambiente de trabalho, o que oferece grandes benefícios ao negócio, como a redução de custos, como o usuário, motivação e produtividade. Em meados de 2011, ouvimos no Brasil o termo "Consumerization", produto da cultura de cópia internacional que evoluiu a partir desse momento a um ritmo acelerado, onde, de acordo com esta prática, liberdade, agilidade e produtividade dos usuários e a organização também trazem riscos, merece atenção. Esses riscos enfrentados por empresas e funcionários podem levar a perdas e riscos para a aplicação bem sucedida do consumo corporativo. O desafio, portanto, é conciliar essa tendência com o trabalho seguro, a responsabilidade do setor de TI, a satisfação dos funcionários no desempenho de sua função e a segurança dos executivos em termos de tráfego de arquivos. e dados da empresa (REZENDE, ABREU, 2013).

Para que BYOD seja implementado no ambiente empresarial, é necessária uma infraestrutura adequada para fornecer o suporte necessário quando necessário: alta maturidade, política de segurança organizacional, informação bem desenvolvida, setor jurídico ativo. Um conjunto de um setor de gerenciamento de RH bem treinado, uma estrutura de suporte apropriada e uma equipe de trabalho em tecnologia da informação e, à medida que essa tendência se torna prática, torna-se uma ferramenta para operações do dia-a-dia e monitoramento contínuo. A informação é o bem mais valioso de uma organização. Garantir que a informação esteja devidamente protegida é essencial para sua sobrevivência. A informação é um recurso importante da organização, independentemente do formato (FONTES, 2006).

A segurança da informação deve ser gerenciada pela organização, que sempre tenta garantir suas principais características: confidencialidade: esta é a garantia de que a informação só será acessível para aqueles que possuem as permissões necessárias (FERREIRA, ARAÚJO, 2008). A falha ao fazê-lo pode resultar em acesso não autorizado, modificação ou mesmo roubo de informações; disponibilidade: esta é a garantia de que a informação estará sempre disponível para as pessoas que o solicitam. A falta de fazê-lo pode resultar em paralisia parcial ou total dos serviços essenciais para a sobrevivência da organização; autenticidade: é garantia de que a informação recebida foi enviada pelo remetente real. A falha ao fazê-lo pode criar vulnerabilidade aos ataques de roubo de identidade e ao homem no meio.

Sabendo que essa informação é o bem mais valioso de uma organização, é extremamente importante protegê-la. Há casos de ataques e roubo de informações e invasão por meios eletrônicos. Uma organização com um Sistema de Gerenciamento de Segurança da Informação (ISMS) pode fornecer maior segurança de informações. Um ISMS efetivo deve ter um setor de TI dedicado com profissionais qualificados, uma política de gerenciamento e segurança bem definida e implementada, funções e responsabilidades bem definidas e um gerente experiente. O gerente deve ser um profissional que tenha a visão e a compreensão de toda a organização e as atividades que acontecem lá. Uma vez que a pessoa responsável pela segurança da informação possui uma ampla base de conhecimento, a criação e implementação de diretrizes torna-se mais específica (FONTES, 2006).

A segurança existe em uma variedade de cenários e é uma preocupação para pessoas e empresas, não é uma adição fácil a uma necessidade. A segurança cobre várias áreas da empresa, cada uma com seus próprios riscos, ameaças potenciais, controles aplicáveis e soluções de segurança que minimizam a extensão da exposição em que a atividade é visível, para garantir a segurança da empresa. Informações: seu bem mais importante. A informação é um dado (ou valores) associados a um conceito claro e inequívoco e ao conhecimento de todos os envolvidos, que é acompanhado por uma referência para o efeito de comparação e pode trazer vantagens competitivas para a organização. Design e referências geralmente não estão associados aos dados relevantes, mas deve ser assegurado que todos os interessados nesta informação tenham o número mínimo de conceitos e referências. Os dados que não são úteis para uma pessoa ou organização não são informações e podem ser rejeitados (FOINA, 2009).

A informação que foi circulada com segurança até algum tempo antes do aparecimento desta onda tecnológica foi interpretada como simples, pois os documentos nos jornais poderiam ser armazenados fisicamente em arquivos, mas com o advento das TICs, a maioria dos computadores se conecta à Internet e a comunicação ocorre ao enviar e receber dados digitais que correspondem a uma atração para usuários mal-intencionados. Não é suficiente, também existem várias situações de incerteza que podem afetar sistemas de informação, como incêndio, inundações, problemas elétricos, poeira, fraude, uso indevido de sistemas, engenharia social, guerras, sequestros e outros. A segurança da informação é um conjunto de políticas, regras, procedimentos, políticas e outras medidas para proteger os recursos de informação que permitem que as atividades e tarefas da organização sejam realizadas. A segurança da informação surgiu para minimizar os riscos associados ao uso de recursos de informação para

garantir que a informação seja acessível apenas para pessoas autorizadas para proteger a precisão e integridade das informações e métodos de divulgação (FONTES, 2006).

A tecnologia torna-se o principal instrumento ao serviço do homem e não é mais a variável independente e dominante que determina tanto a estrutura como o comportamento das organizações, como foi o caso nos dois períodos industriais precedentes. Para o autor, a tecnologia que antes se considerava o acessório dominante agora está sendo analisada como um fator organizacional estratégico porque agora é responsável por armazenar, restaurar, processar, disseminar e disseminar a informação a que deve ser aplicada com a segurança necessária para o seu tráfego (CHIAVENATO, 2014).

Os benefícios do BYOD são infinitos: você trabalha com seu software e aplicativos favoritos até que você possa trabalhar de qualquer lugar com uma conexão com a Internet, por exemplo, para acessar os recursos da empresa para uma VPN. A maior vantagem, no entanto, é a satisfação dos funcionários. A satisfação e o envolvimento do colaborador são alcançados permitindo que a empresa use seus dispositivos pessoais para fins profissionais, o que funciona com maior satisfação e, ao mesmo tempo, beneficia a empresa com uma significativa redução de custos e um aumento significativo nos custos. A mobilidade permite que os funcionários trabalhem de qualquer lugar, a qualquer hora, em qualquer lugar através do seu dispositivo, e acessem seus documentos. Entre as desvantagens, a segurança é unânime. O uso de dispositivos móveis cresceu exponencialmente, mas a segurança desses dispositivos não acompanhou a demanda. Cerca de 4% dos smartphones são roubados ou perdidos a cada ano, e esses dispositivos roubados também podem abrir uma vulnerabilidade e outras oportunidades prejudiciais, expondo dados corporativos sensíveis (KEYES, 2013).

As questões de segurança e comunicação da informação (CIS) são destacadas como uma grande preocupação pela adoção do BYOD por todos os especialistas entrevistados no teste de materiais para o tópico em consideração. É natural que isso seja assim, que as organizações que já estão usando o BYOD e aqueles que querem assumi-lo são conscientes de que ainda não estão cobertas e estão resolvendo todas as vulnerabilidades e ameaças que possam pôr em perigo seu patrimônio mais valioso (informação) quando o modo BYOD é adotado (DODT, 2013).

BYOD para uso pessoal e profissional, no qual os dispositivos móveis pessoais dos funcionários podem ser conectados à rede corporativa, apresenta problemas de segurança, uma vez que todos estão cansados de saber que o usuário é a “conexão fraca no fluxo”, tanto para o puro e simples ignorância de alguns dos riscos associados ao acesso a redes e ambientes

desprotegidos e desprotegidos, bem como a outros usuários mal-intencionados que utilizam seus conhecimentos para praticar atos ilegais através dos direitos de acesso para os quais a empresa lhes concede seu trabalho (GARANHANI, 2013).

O acesso a redes sociais por alguns funcionários da BYOD que desconhecem os riscos que enfrentam ao visitar esses sites também é uma preocupação. Esses funcionários são usuários dessas redes populares, onde a maioria dos usuários da Internet não tem riscos de segurança. Um provedor antivírus (Panda Security) vazou o 1º Índice Anual de Risco em redes sociais das PME em março e descobriu que 78% das empresas pesquisadas usam ferramentas como *Facebook, Twitte*r e *LinkedIn* para apoiar a estratégia da empresa. Os resultados do estudo mostram que o *Facebook* é o maior responsável por infecções de *malware* (71,6%) e violações de dados em 73,2%. Em empresas que relataram perdas econômicas devido a falhas de dados dos funcionários, o *Facebook* voltou a estar em 62%. O estudo também mostra que os principais riscos das mídias sociais são o roubo de identidade, infecção e a vulnerabilidade da própria ferramenta. Panda descobriu que 77% dos funcionários usam redes sociais durante o horário de trabalho. Situação que pode causar o intercâmbio de informações confidenciais (OLIVEIRA; SOARES, 2011).

Outra pesquisa recente, desenvolvida pela *Trustwave*, uma conhecida empresa de segurança informática, por meio de seu relatório *'2013 Trustwave Global Security Report'*, releva informações importantes relacionados ao BYOD (TRUSTWAVE, 2013): mais de 450 investigações de incidentes foram realizadas, adicionando dois milhões de varreduras de vulnerabilidades, 400 violações de dados da Web e mais de 20 bilhões de e-mails de dados; o relatório observa que o acesso remoto foi mais uma vez a metodologia mais comumente utilizada para violação de dados em 2012, representando 47% dos ataques analisados. Em 2012, o número de casos de *malware* móvel aumentou em 400%.

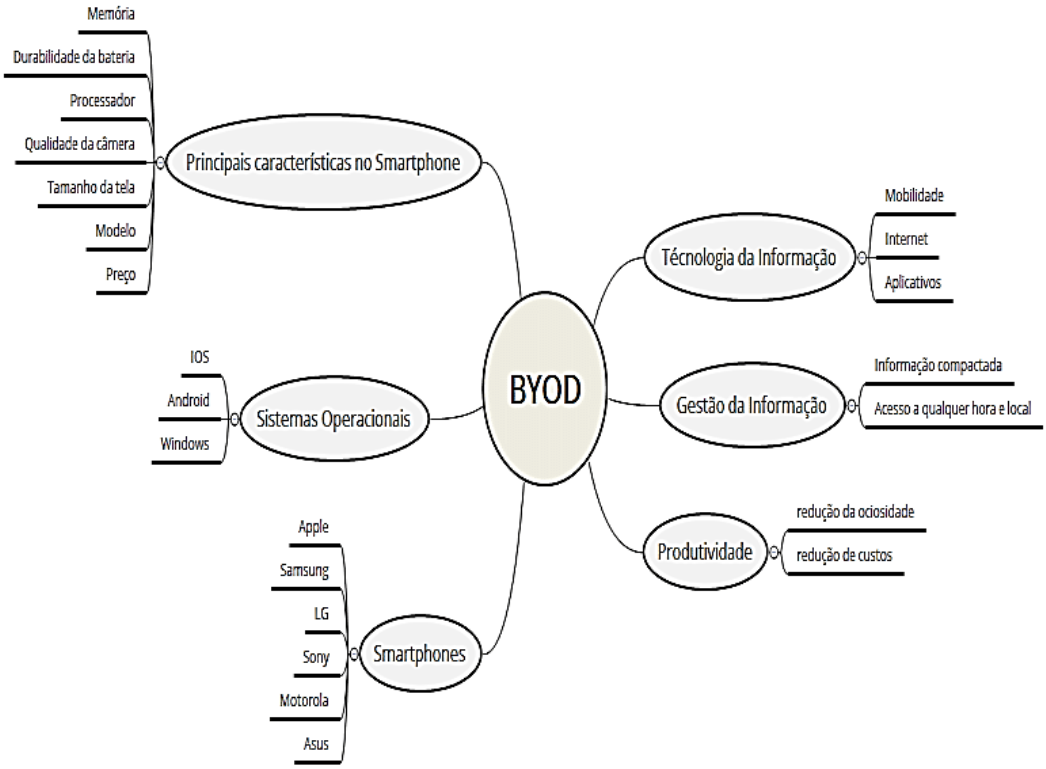
O fato é que, com o BYOD, o colaborador (o usuário) mantém a faca e o queijo na mão, ou seja, privilégios e facilidades concedidos para usar seu dispositivo móvel na rede da organização quando e como quiser. Por este e outros motivos, para adotar uma estratégia de pensamento BYOD sem muito esforço, os especialistas concordam que o desenvolvimento de uma política de uso de BYOD para a proteção de dados confidenciais é essencial para minimizar os riscos neste modo de trabalho (DODT, 2013).

As questões relacionadas à segurança da informação sob o conceito de BYOD são extremamente importantes, havendo a necessidade de implementar políticas para BYOD para

monitorar o acesso dos usuários, verificações de segurança, monitoramento e auditoria para a gestão efetiva de BYOD de gastos, entre outros (GARANHANI, 2013).

Ao introduzir BYOD, é altamente recomendável avaliar os riscos e as vulnerabilidades que podem surgir diante dessa realidade. Como alternativa ao fornecimento de recursos que agregam segurança à rede corporativa com BYOD, recomenda-se que a virtualização do equipamento onde as informações sejam processadas sem a necessidade de armazenamento local. Todas as informações e aplicativos estão no servidor da empresa (SANTOS, 2012).

Com base nesse contexto, a presente pesquisa analisou os principais aspectos relacionados a segurança em redes de computadores com ênfase no conceito BYOD, destacando o seguinte questionamento: quais são as principais vantagens e desvantagens para a segurança da informação das organizações que adotam o conceito de BYOD? Fazemos uma análise da figura abaixo para conclusão das vantagens sobre a adoção.



Fonte: Santos et al. (2018).

Podemos dizer que reduzir o custo em implantação de equipamentos de infraestrutura, pode gerar um ganho essencial na produtividade da organização.

Em algumas ocasiões o colaborador tem a possibilidade de estender seu alcance de trabalho em casa, gerando assim uma comodidade maior para organização.

Além de ganhos na produtividade, as organizações podem também ter menos ocorrências em atestado médico devido ao alto índice de estresse proporcionado devido à falta de equipamentos adequados para desenvolvimento das atividades laboral.

Na utilização do termo BYOD a mobilidade do colaborador ter acesso de qualquer lugar, utilizando como nova forma de trabalho o chamado *home office*, regulamentado pela recente reforma trabalhista, com o advento da *cloud computing* (ou computação em nuvem) esse método, portanto, pode ser útil para as empresas.

Obviamente podemos dizer que o avanço dessas tecnologias, podem de certa forma trazer alguns desconfortos as organizações. O que se pode dizer que optar por usar essa nova modalidade tecnológica, pode ter um custo muitas vezes alto para as organizações.

Pois para que de certa forma o colaborador possa se utilizar da BYOD, ele precisara ter uma infraestrutura adequada dentro das organizações, mudança podem acontecer também quando se abre as portas para dispositivos pessoais, uma delas a falta de segurança de dados, pois nem todos colaboradores detém de conhecimentos em informática suficiente para, ter em seus dispositivos mecanismos de segurança.

Outra questão a ser pautada como desvantagem é, um desconforto entre colaboradores que não tem o mesmo poder aquisitivo para dispor de um dispositivo à altura, uma certa inveja pode acontecer. Competividade entre colaboradores devido a performance de equipamentos.

Contudo se pode dizer que para as organizações a adoção deste modelo, trará um ganho em potencial de produção e aumento de harmonia no ambiente empresarial, fortalecendo os lanços entre as organizações e seus colaboradores.

CONCLUSÃO

A presente pesquisa analisou as principais vantagens e desvantagens para a segurança da informação perante a adoção do conceito BYOD nas organizações, onde verificou-se que tal conceito pode trazer avanços importantes nas organizações, desde sejam adotadas as devidas medidas de segurança da informação, evitando eventuais riscos para a organização.

Segurança em redes de computadores é um problema complexo. Este é um desafio para as empresas que desejam gerar lucros, economizar tempo e reduzir custos, tornando-os uma ferramenta de infraestrutura importante. Os procedimentos e recursos de segurança devem ser considerados uma prioridade e, portanto, devem ser constantemente reavaliados nas empresas. Neste cenário amigável e hostil do sistema de segurança, os profissionais devem reconhecer os limites e tomar as decisões apropriadas para resolvê-los.

O objetivo de reavaliar a segurança nas organizações impostas pela nova realidade global não deve ser o foco. Por outro lado, não é desejável que as decisões sejam tomadas com base em análises superficiais ou políticas extremas e inflexíveis baseadas no medo e na insegurança.

A introdução de medidas de segurança é, sem dúvida, um trabalho de longo prazo e prudente, exatamente o oposto do tipo de trabalho que a maioria dos técnicos fazem. Isso é essencial para a segurança da instituição.

Manter os *firewalls* eficientes e compatíveis com medidas de segurança também é um excelente trabalho. Todos os sistemas de TI que filtram o conteúdo devem refletir o gerenciamento que espera cumprir com a Política de Uso da Internet e minimizar o potencial de ataque, invasão e perda de informação, preservando a integridade e a reputação da instituição.

Os consumidores, ou BYOD, são a tendência promovida através do uso de tecnologias simples, acessíveis e acessíveis que permitem às empresas que usam este modelo permitir que seus funcionários trabalhem em qualquer lugar, a qualquer momento, com dispositivos conectados à rede e aos sistemas informações conectadas. O objetivo deste artigo foi analisar o quão útil é para a empresa assumir a consumação no negócio, o que é permitir que seus funcionários usem seu dispositivo pessoal dentro da organização.

Se a empresa autorizar o empregado a usar o próprio dispositivo, é importante e essencial preparar uma boa política de segurança porque a mobilidade do dispositivo é, ao mesmo tempo, benéfica para a organização e os funcionários à medida que a informação sensível está comprometida da empresa.

A pesquisa mostrou que, se a empresa aplicar uma boa política de segurança, aplica uma política de consumação, desenvolve uma campanha de disseminação, estabelece regras que estabelecem limites entre o uso pessoal e profissional, e será benéfico para as empresas que se consomem. À medida que o funcionário trabalha mais motivado, tem mais produtividade, reduz custos e mobilidade e acelera a forma como as pessoas trabalham.

Sugere-se, ainda, que outros estudos sejam desenvolvidos para discutir e fortalecer conceitos e posicionamentos referente à segurança da informação em relação ao conceito BYOD nas organizações, levando-se em consideração o avanço das TICs – Tecnologias da Informação e da Comunicação, bem como a evolução da sociedade e do mercado.

REFERÊNCIAS

BEAL, Adriana. **Segurança da Informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações – São Paulo: Atlas, 2005.

BERNERS-LEE, T.; FIELDING, R.; IRVINE, U. C.; MASINTER, L. **Uniform Resource Identifiers (URI):** Generic Syntax. The Internet Engineering Task Force - IETF / Network Working Group, 1998. Disponível em: < http://www.ietf.org/rfc/rfc2396.txt >. Acesso em: 27 de fevereiro de 2020.

BRADLEY, Jospeh; LOUCKS, Jeff; MACAULAY, James; MEDCALF, Richard; BUCKLEW, Lauren. ***BYOD:*** *una perspectiva global Cómo aprovechar la innovación liderada por los empleados.* CISCO Internet Business Solutions Group (IBSG). San Jose: CISCO, 2012. Disponível em: < https://www.cisco.com/c/dam/en_us/about/ac79/docs/re/byod/BYOD_Horizons-Global_LAS.pdf >. Acesso em: 27 de fevereiro de 2020.

CARRERA, Filipe. **Comunicar 2.0:** A arte de bem comunicar no século XXI. Lisboa: Edições Silabo, 2012.

CASTELLS, Manuel. **A Galáxia Internet:** Reflexões sobre Internet, Negócios e Sociedade. Lisboa: Fundação Calouste Gulbenkian, 2004.

CEPTRO. **Estudos sobre a Web.** CEPTRO – Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações. Disponível em: < http://www.ceptro.br/CEPTRO/MenuCEPTROSPCensoWeb >. Acesso em: 27 de fevereiro de 2020.

CHIAVENATO, Idalberto. **Introdução à Teoria Geral da Administração.** 9. ed. Rio de Janeiro: Elsevier, 2014.

COMPUTERWORLD. **Consumerização:** aliada ou inimiga da equipe de TI? Artigo publicado em 5 de outubro de 2011. Disponível em: < http://computerworld.com.br/tecnologia/2011/10/05/consumerizacao-aliada-ou-inimiga-da-equipe-de-ti/ >. Acesso em: 27 de fevereiro de 2020.

DEMETRIO, Rinaldo. **Internet.** São Paulo: Érica, 2001.

DEMO, Pedro. **Aprendizagens e Novas Tecnologias.** Disponível em: < http://www.pucrs.br/famat/viali/doutorado/ptic/textos/80-388-1-PB.pdf >. Acesso em: 27 de fevereiro de 2020.

DIGITAL DISCOVERY. **A Evolução da Web 1.0 para a Web 2.0.** Disponível em: < http://digitaldiscovery.eu/a-evolucao-da-web-1-0-e-a-web-2-0/ >. Acesso em: 27 de fevereiro de 2020.

DODT, Cláudio. **Consumerização, BYOD e MDM:** Indo além da sopa de letrinhas da mobilidade. Artigo publicado em 23 de maio de 2013. Disponível em: <

http://claudiododt.com/pt/consumerizacao-byod-e-mdm-indo-alem-da-sopa-de-letrinhas-da-mobilidade/ >. Acesso em: 27 de fevereiro de 2020.
DRUCKER, Peter Ferdinand. **Administrando em Tempos de Grandes Mudanças.** 3. ed. São Paulo: Pioneira, 1996.

FARIA, Fabio. **Prefácio.** In: ALBERTIN, Alberto Luiz; MOURA, Rosa Maria de (Organizadores). Tecnologia de Informação. São Paulo: Atlas, 2004.

FERNANDES, Almir. **Administração Inteligente.** São Paulo: Futura, 2001.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de segurança da informação:** guia prático para elaboração e implementação. 2. ed. Rio de Janeiro: Ciência Moderna, 2008.

FOINA, P. R. **Tecnologia de Informação:** Planejamento e Gestão. 2. ed., 339 p. ISBN: 9788522443727. São Paulo: Atlas, 2009.

FONTES, Edison Luiz Gonçalves. **Segurança da Informação:** o usuário faz a diferença. São Paulo: Saraiva, 2006.

FORREST, Brady. ***Controversy about our "Web 2.0" Service Mark.*** Artigo publicado em 25 de maio de 2007, originalmente em inglês, no Portal O´Reilly Radar. Disponível em: < http://radar.oreilly.com/2006/05/controversy-about-our-web-20-s.html >. Acesso em: 27 de fevereiro de 2020.

GARANHANI, Bruno. ***BYOD:*** *Bring Your Own Device.* 37 f. 2013. Monografia (Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Rede). Programa de Pós-Graduação em Tecnologia. Universidade Tecnológica Federal do Paraná. Curitiba: Universidade Tecnológica Federal do Paraná, 2013. Disponível em: < http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/2520/1/CT_GESER_III_2013_05.pdf >. Acesso em: 27 de fevereiro de 2020.

IMBERNÓN, Francisco. **Formação Docente e Profissional:** Formar-se para a Mudança e a Incerteza. 7. ed. São Paulo: Cortez, 2010.

JURAN, Joseph M.; GRYNA, Frank M. **Controle da Qualidade *Handbook*:** Conceitos, Políticas e Filosofia da Qualidade. São Paulo: Makron, McGraw-Hill, 1991.

KEYES, Jessica. ***Bring Your Own Devices (BYOD):*** *Survival Guide.* 451 p. ISBN: 9781466565036. CRC Press, 2013.

KUROSE, James F. **Redes de computadores e a Internet**: uma aboradagem top-down / James F. Kurose e Keith W. Ross; tradução Opportunity translations; revisão técnica Wagner Zucchi. – 5. Ed. Pearson Education do Brasil – São Paulo: Addison Wesley, 2010.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Metodologia do Trabalho Científico.** 7. ed. São Paulo: Atlas, 2007.

LERMAN, LAURA VISINTAINER. **Análise Sobre O Uso Do Byod No Sebrae / Rs**: Um Estudo De Caso, 2013. Disponível em: < http://revistaseletronicas.pucrs.br/ojs/index.php/graduacao/article/view/19334/12297 >. Acesso em: 28 de fevereiro de 2020.

LÉVY, Pierre. **Inteligência Coletiva:** Por Uma Antropologia do Ciberespaço. Trad. L. Rouanet. São Paulo: Loyola, 1998.

LUCKESI, C. C.; PASSOS, E. S. **Introdução à Filosofia:** Aprendendo a Pensar. São Paulo: Cortez, 1996.

LÜDKE, Menga; ANDRÉ, Marli E. D. **Pesquisa em Educação:** Abordagens Qualitativas. 10. reimp. São Paulo: EPU, 2007.

LYRA, Mauricio Rocha. **Governança da Segurança da Informação**. Edição do Autor – Brasília, 2015.

MARTINS, G. A.; PINTO, R. L. **Manual para Elaboração de Trabalhos Acadêmicos.** São Paulo: Atlas, 2001.

MDN. **Introdução ao HTML.** MDN – Mozilla Developer Network. Uma breve história da HTML. Disponível em: < https://developer.mozilla.org/pt-BR/docs/HTML/Introduction >. Acesso em: 27 de fevereiro de 2020.

MEYER, Marilyn; BABER, Roberta; PFAFFENBERGER, Bryan. **Nosso Futuro e o Computador.** Porto Alegre: Bookman, 2000.

MORAN, José Manuel; MASSETTO, Marcos T.; BEHRENS, Marilda Aparecida. **Novas tecnologias e mediações pedagógicas.** Campinas: Papirus, 2012.

NETO, Everaldo. **Evolução da Web.** Histórico. Disponível em: < http://slideplayer.com.br/slide/3423438/ >. Acesso em: 27 de fevereiro de 2020.

OLIVEIRA, Débora, SOARES, Edileuza. **Mobilidade, redes sociais e nuvem impactam a forma tradicional de proteger as informações estratégicas.** Elas estão em toda a parte. Como blindá-las? Artigo publicado em 5 de maio de 2011. Disponível em: < https://issuu.com/nowdigital/docs/cw536-web > Acesso em: 27 de fevereiro de 2020.

PINTO, Gilmar José Silva; GRAEML, Alexandre Reis. **Alinhamento entre Tecnologia da Informação e Negócios:** O Caso de uma Cooperativa Médica no Paraná. v. 18, n. 2, p. 259-274, abr./jun. DOI: 10.5700/rege 426. São Paulo: REGE, 2011. Disponível em: < https://ac.els-cdn.com/S1809227616303708/1-s2.0-S1809227616303708-main.pdf?_tid=f2d57898-cec8-11e7-b3ec-00000aab0f6c&acdnat=1511274992_22b0c1f3a9596372fbfe043e4d366d33 > . Acesso em: 27 de fevereiro de 2020.

REZENDE, Denis Alcides; ABREU, Aline França de. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais.** O papel estratégico da Informação e dos Sistemas de Informação nas Empresas. 9. ed. rev. ampl. São Paulo: Atlas, 2013.

ROMEIRO FILHO, Eduardo. **Projeto do Produto.** Apostila do curso. Segundo semestre de 2006. 8. ed. Belo Horizonte: LIDEP/DEP/EE/UFMG, 2006. Disponível em: < http://www.dep.ufmg.br/wp-content/uploads/2015/01/apostilaprodutoufmg.pdf >. Acesso em: 27 de fevereiro de 2020.

SANTOS, Tácito. **BYOD:** como controlar dispositivos móveis nas empresas? Artigo publicado em 6 de abril de 2012. Disponível em: < http://www.administradores.com.br/noticias/negocios/byod-como-controlar-dispositivos-moveis-nas-empresas/54038/ >. Acesso em: 27 de fevereiro de 2020.

SENGE, Peter M.; KLEINER, Art; ROBERTS, Charlotte; ROSS, Richard; ROTH, George; SMITH, Bryan. **A Dança das Mudanças:** os desafios de manter o crescimento e o sucesso em organizações que aprendem. 7. ed. Rio de Janeiro: Campus, 1999.

STAIR, Ralph M.; REYNOLDS, George W. **Princípios de Sistemas de Informação.** Trad. Noveritis do Brasil. Rev. Téc. Tânia Fátima Calvi Tait. 11. ed. Trilha / Cengage Learning, 2015. Disponível em: < http://www.patricialucas.com.br/file/2017/02/Livro-Sistemas-de-informa%C3%A7%C3%A3o.pdf >. Acesso em: 27 de fevereiro de 2020.

SVEIBY, Karl Erik. **A Nova Riqueza das Organizações.** Rio de Janeiro: Campus, 1998.
TRUSTWAVE. ***2013 Trustwave Global Security Report.*** Research Report. February 21, 2013. Trustwave Holdings, Inc., 2013. Disponível em: < https://www.trustwave.com/Resources/Library/Documents/2013-Trustwave-Global-Security-Report/ >. Acesso em: 27 de fevereiro de 2020.

W3C BRASIL. **Sobre o W3C.** Disponível em: < http://www.w3c.br/Sobre/ >. Acesso em: 27 de fevereiro de 2020.

Autores:

Ideir Coto
ideir.coto@ifro.edu.br
Instituto Federal de Rondônia
Brasil
Mestrado em Administração pela Universidade Paulista/UNIP (2021). Pós-graduado em Educação Profissional e Tecnológica pela Cetiqt - RJ (2014), Pós-graduado em Metodologia e Didática do Ensino Superior pela UNESC - RO (2012), Graduado em Analise e Desenvolvimento de Sistemas pela Universidade Nove de Julho - SP (2011)

Pedro Vinícius Rodrigues Dias
pedrovinny2@gmail.com
IEAA - UFAM
Brasil
Analista de Sistemas pela São Lucas Ji-Paraná-RO e Pós Graduado em Ciência de Dados pela UNIASSELVI, Atuou como Analista de Sistemas na Unimed Ji-Paraná, docente no Instituto Federal de Rondônia e atualmente é Técnico em Tecnologia da Informação na Universidade Federal do Amazonas (UFAM).