FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Myke Monteiro de Barros

BYOD: *BRING YOUR OWN DEVICE*

Estudo sobre a utilização de dispositivos móveis em ambientes corporativos

Americana, SP

2018

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Myke Monteiro de Barros

BYOD: *BRING YOUR OWN DEVICE*

Estudo sobre a utilização de dispositivos móveis em ambientes corporativos

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação da Prof. Benedito Aparecido Cruz.

Área de concentração: Segurança da Informação.

Americana, SP

2018

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

B279b BARROS, Myke Monteiro de

BYOD - bring your own device: estudo sobre a utilização de dispositivos móveis em ambientes corporativos. / Myke Monteiro de Barros. – Americana, 2018.

53f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Benedito Aparecido Cruz

1 Dispositivos móveis – aplicativos I. CRUZ, Benedito Aparecido II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU:681.519

Myke Monteiro de Barros

BYOD: *BRING YOUR OWN DEVICE*

Estudo sobre a utilização de dispositivos móveis em ambientes corporativos

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 26 de junho de 2018.

Banca Examinadora:

Benedito Aparecido Cruz (Presidente)
Mestre
Fatec Americana

Acácia de Fátima Ventura (Membro)
Doutora
Fatec Americana

Edson Roberto Gaseta (Membro)
Especialista
Fatec Americana

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus que me deu a capacidade de chegar onde estou hoje, guiando-me com sabedoria nos caminhos pelos quais passei.

Agradeço à minha mãe Maria de Lourdes, pai Aldair, avó Armelinda e irmão Vinicius que me deram educação e estrutura para chegar até aqui.

Meus sinceros agradecimentos aos professores que me ensinaram, orientaram e corrigiram quando necessário.

Ao meu orientador por todo o apoio e confiança, por me auxiliar com seu conhecimento e experiência.

A professora Maria Cristina Aranda que me auxiliou constantemente na solução de dúvidas.

Com isso pude crescer como acadêmico e profissionalmente.

DEDICATÓRIA

Aos meus familiares, amigos, professores e a todos que sempre me apoiaram nessa trajetória.

RESUMO

O presente estudo tem como objetivo dissertar sobre os conceitos e as finalidades dos fenômenos de consumerização, BYOD (*Bring Your Own Device*) e políticas de segurança adotadas em organizações, bem como a relação intrínseca entre estes temas. Por meio da consumerização, dispositivos eletrônicos portáteis tais como *notebooks* e *smartphones* deixaram de ser artigos restritos a determinados nichos profissionais e governamentais e passaram a ser ofertados de maneira simples, ágil e em ampla escala ao público em geral. Este advento atenuou a linha divisória entre o público e o privado, tanto em termos de patrimônio físico quanto de capital intelectual, acabando por fundir parcialmente o ambiente organizacional ao particular. Já não é possível permitir a livre atuação de usuários em uma rede corporativa sem adotar práticas de proteção adequadas aos dados e informações que por ela transitam. Falhas de segurança, intencionais ou não, podem comprometer todos os níveis administrativos de uma instituição, gerando desde pequenos erros solucionáveis até transtornos permanentes capazes de arruinar uma empresa por completo. Além da introdução aos assuntos mencionados, serão apresentados os benefícios e as desvantagens decorrentes do uso dos dispositivos móveis e as estratégias envolvidas na implementação da prática nas organizações, bem como políticas de segurança que podem ser utilizadas para garantir a integridade das informações corporativas. O estudo de caso foi desenvolvido junto a usuários potenciais e efetivos da tecnologia BYOD, demonstrando a inevitabilidade do crescimento desta atividade e, portanto, da necessidade de desenvolver um estudo competente sobre o assunto.

Palavras Chave: Consumerização; Dispositivos Móveis; Segurança da Informação.

ABSTRACT

The present study aims to discuss the concepts and purposes of consumerization phenomena, BYOD (Bring Your Own Device) and security policies adopted in organizations, as well as the intrinsic relationship between these themes. Through consumerization, portable electronic devices such as notebooks and smartphones have ceased to be articles restricted to certain professional and governmental niches and have been offered in a simple, agile and wide-scale manner to the general public. This advent attenuated the dividing line between public and private, both in terms of physical assets and intellectual capital, eventually merging the organizational environment with the individual. It is no longer possible to allow the free operation of users in a corporate network without adopting adequate protection practices to the data and information that passes through it. Security failures, whether intentional or not, can compromise all administrative levels of an institution, ranging from small, problem-solving errors to permanent disruptions that can ruin a business completely. In addition to the introduction to the issues mentioned, the benefits and disadvantages of using mobile devices and the strategies involved in implementing the practice in organizations will be presented, as well as security policies that can be used to ensure the integrity of corporate information. The case study was developed with potential and effective users of BYOD technology, demonstrating the inevitability of this activity growth and, therefore, the need to develop a competent study on the subject.

Keywords: *Consumerization; Mobile Devices; Information Security.*

Sumário

LISTA DE FIGURAS

LISTA DE GRÁFICOS E TABELAS

LISTA DE ABREVIATURAS E SIGLAS

BYOD – Bring Your Own Device

CETIC – Centro de Estudos sobre as Tecnologias da Informação e Comunicação

E-MAIL – Eletronic Mail

ERP – Enterprise Resource Planning

IBSG – Internet Business Solutions Group

IP – Internet Protocol

ISO – International Standards Organization

ITIL – Information Technology Infrastructure Library

MALWARE – Malicious Software

MDM – Mobile Device Management

NAC – Network Access Control

TI – Tecnologia da Informação

VRF – Virtual Routingand Forwarding

INTRODUÇÃO

A maioria massiva dos produtos baseados em tecnologia tiveram como origem a satisfação de necessidades governamentais e corporativas. Equipamentos que atualmente estão presentes em todas as residências, como calculadoras e telefones, surgiram em mercados de negócios e somente com o tempo se tornaram dominados pelo consumidor em grande volume, pois tiveram seus custos de produção e comercialização reduzidos, bem como foram adaptados para o uso cotidiano.

"A reorientação dos projetos de produtos e serviços com foco em vendas de empresa para empresa ou empresa para governo para o foco do usuário final como consumidor individual é chamada de consumerização" (NEAL; TAILOR, 2004, p. 2). Embora este fenômeno já exista há décadas, o termo foi utilizado formalmente pela primeira vez em 2004, em um artigo resultante do fórum Leading Edge, evento que reúne especialistas em tecnologia da informação de todo o mundo.

O avanço contínuo do processo de consumerização tem permitido que milhões de pessoas tenham acesso a dispositivos móveis como *notebooks, smartphones* e *tablets*. De acordo com a Fundação Getúlio Vargas (FGV, 2017, p. 7), até o final do presente ano o Brasil terá um *smartphone* para cada habitante, alcançando 208 milhões de aparelhos em uso. Ainda segundo a instituição, o número de *notebooks* será de quatro para cada cinco habitantes.

Os sistemas operacionais destes equipamentos disponibilizam ao usuário uma gama infinita de programas e aplicativos que podem ser utilizados para os fins mais diversos, desde planilhas para controle do orçamento doméstico até *softwares* gráficos para a produção de conteúdos artísticos. Em meio a todas estas possibilidades, agrega-se um recurso de importância imensurável: a internet.

Em pesquisa divulgada no ano passado, a CETIC (2015, p. 128) demonstrou que 54% dos lares brasileiros possuem acesso à internet, sendo que 14% das conexões são realizadas através de dispositivos móveis. O relatório também afirmou que os *smartphones* ultrapassaram os *notebooks* como principal meio de acesso à

rede, alcançando 69% dos internautas, e que a média de utilização é de quase 5 horas diárias. Dentro desta estatística de uso, cerca de 2,1 horas são dispendidas no ambiente corporativo.

Durante a última década, tornou-se comum para os trabalhadores possuírem equipamentos eletrônicos móveis de utilização dupla, ou seja, para uso particular e profissional. Este hábito é conhecido como BYOD, *Bring Your Own Device*, termo que em tradução livre significa “traga seu próprio dispositivo”. O constante crescimento desta prática deve-se não somente ao aumento da popularidade dos dispositivos, mas principalmente ao ganho de produtividade e eficiência pela sincronia entre as esferas corporativas e pessoais.

Borrett (2013, p. 5-6) afirma que 69% das companhias permitem que seus colaboradores utilizem dispositivos pessoais para executar tarefas corporativas. Harris (2012, p. 101), entretanto, ressalta que 76% destas empresas só autorizam o uso mediante equipamento monitorado pela própria organização, ficando sob responsabilidade do empregado enquanto este estiver ligado ao quadro de funcionários, e com a condição de inspeção e confisco sem prévio aviso. Esta alta porcentagem demonstra a preocupação das organizações em manter a segurança de suas informações.

Os resultados de uma pesquisa realizada com 600 gestores de tecnologia da informação dos Estados Unidos indicam que 85% dos tomadores de decisão em TI disseram que suas empresas apoiam o BYOD de alguma forma. Igualmente importante foi a atitude deles em relação ao BYOD. Sem minimizar os desafios impostos pela implementação da prática, 72% o consideraram ‘bastante’ ou ‘extremamente’ positivo para os departamentos de tecnologia (IBSG,2012, p. 2).

Diante do contraponto entre as estatísticas apresentadas, este trabalho voltou-se para a seguinte questão: Existe a possibilidade de se implementar o BYOD em uma organização sem arriscar a segurança das informações corporativas.

Foram analisadas e estruturadas etapas de implementação de dispositivos móveis nas organizações, bem como apresentadas políticas de segurança que garantam a integridade das informações organizacionais.

O objetivo geral deste estudo consistiu em abordar o conceito de BYOD em redes corporativas, enfatizando a necessidade de implementar corretamente o processo de utilização de dispositivos.

Já os objetivos específicos resumiram-se em três tópicos: a) Fazer um levantamento bibliográfico sobre BYOD em redes corporativos, objetivando garantir a segurança da informação; b) Fazer um estudo de caso, visando compreender o perfil de usuários potenciais e efetivos da tendência BYOD e, c) Apresentar soluções de segurança da informação para assegurar o funcionamento do BYOD, buscando identificar as etapas envolvidas no processo de implementação do BYOD, bem como observar as vantagens e desvantagens decorrentes de tal implementação.

A produção deste trabalho justifica-se pela necessidade de garantir a segurança das informações corporativas durante e após o processo de implementação do BYOD, de modo que este possa continuar sendo aplicado no ambiente de trabalho. A inserção de dispositivos móveis no âmbito corporativo tem-se mostrado altamente benéfica, mas poderá ser descartada caso comprometa o sigilo dos dados ou subverta sua aplicação. Além disso, o estudo mostra-se como objeto compilatório de diversas bibliografias, unindo referências sobre os assuntos de consumerização, BYOD e segurança da informação.

Para a realização deste trabalho, utilizou-se pesquisa exploratória e descritiva. A pesquisa exploratória foi executada através de referencial bibliográfico para o levantamento e a análise do que já foi produzido por especialistas e profissionais a respeito dos assuntos abordados. Por se tratar de um tema atual, a maioria das informações foram retiradas de artigos virtuais, todos devidamente mencionados e abertos à exame no capítulo de referências. Além disto, a pesquisa descritiva deu-se em forma de levantamento de dados por um questionário, para averiguar as opiniões de usuários ativos e potenciais do BYOD.

Este estudo foi estruturado em dois capítulos baseados em pesquisa bibliográfica, sendo que o primeiro conceitua os temas de consumerização, BYOD e os métodos para implementação de dispositivos móveis em redes corporativas, o segundo determina o que é segurança da informação, demonstra políticas de segurança gerais e específicas para garantir a integridade dos dados organizacionais.

A sessão final deste artigo foi desenvolvida com base na análise dos dados obtidos por meio da aplicação de um questionário sobre BYOD, e é seguida pelas considerações finais observadas pelo estudo em geral. Por fim, são apresentadas as referências bibliográficas utilizadas para o desenvolvimento do trabalho.

1 CONSUMERIZAÇÃO E BYOD

O termo consumerização é, equivocadamente, utilizado como sinônimo para BYOD. Ainda que próximos, os conceitos são distintos. O BYOD é uma consequência do processo de consumerização que, por sua vez, vai muito além da inserção de dispositivos móveis no ambiente corporativo. Para melhor compreensão destes fenômenos, faz-se necessário apresenta-los separadamente.

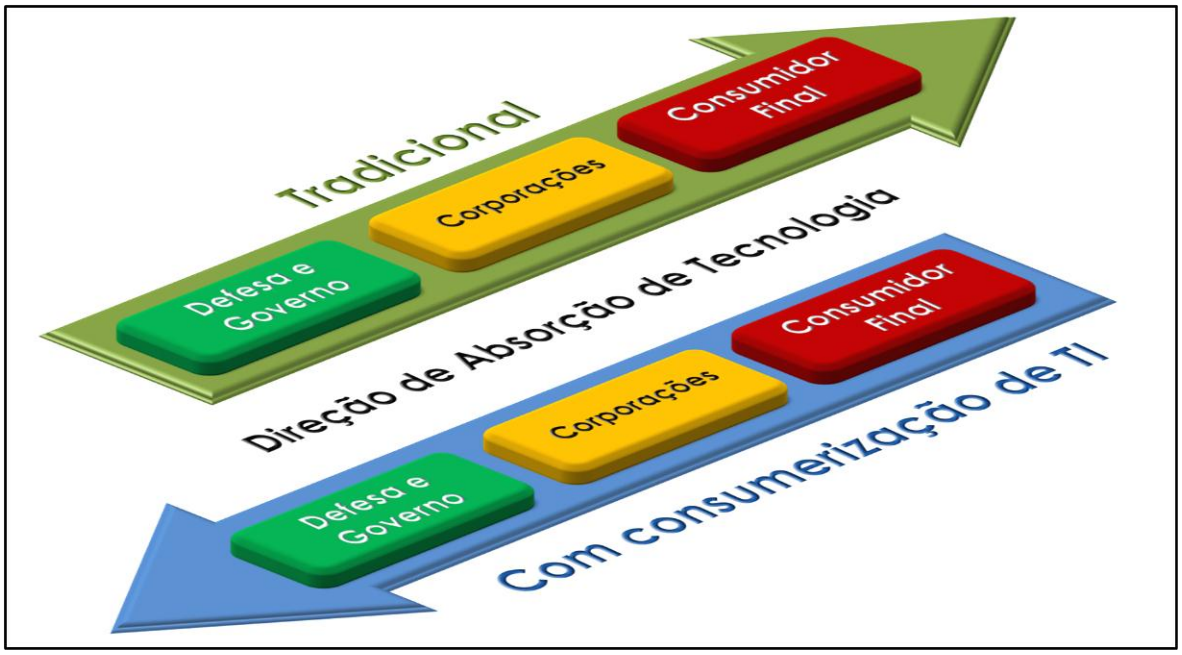
1.1 CONSUMERIZAÇÃO

No início da produção tecnológica, os bens eram direcionados para consumo governamental e do mercado de negócios. Entretanto, a evolução da manufatura expandiu a esfera de utilização destes bens:

> Uma mudança de paradigma ocorreu no mundo da tecnologia. O padrão de evolução tecnológica existente no passado, quando as novidades estavam disponíveis primeiro para as empresas e apenas após alguns anos chegavam ao consumidor residencial, foi invertido. Motivados pelo tamanho do mercado de consumo, os fabricantes de tecnologia passaram a investir mais na criação de produtos para o uso residencial, reduzindo drasticamente o preço de venda e lançando inovações tecnológicas com cada vez mais frequência. Este fenômeno é genericamente conhecido como consumerização (CERIONI, 2012, p. 4).

Segundo Castro e Souza (2015, p. 3), a consumerização quebra o ciclo da inovação tecnológica, no qual os equipamentos eram fabricados primeiramente para fins governamentais, depois para consumidores de grande porte, ou seja, corporações, e por fim para o consumidor em pequena escala. Com o passar dos anos, a direção da produção de bens tecnológicos inverteu-se, tendo a pessoa física como foco, como pode ser observado na Figura 1.

Figura 1 – Fluxo de Absorção de Tecnologia



Fonte: Banerjee (2012, s/p)

O consumidor final como público alvo exigiu adaptações por parte da indústria tecnológica. O usuário deixa de ser um profissional especializado de um ramo específico de atuação e passa a ser um indivíduo leigo que necessita de *interfaces* simples e intuitivas. De acordo com Garanhani (2013, p.10), a consumerização "ajuda a desenvolver dispositivos com plataformas de aplicativos mais inteligentes e serviços personalizados". O mesmo autor argumenta que "fatores como '*clouding'* e redes sociais são alguns dos recursos mais conhecidos dos *mobiles*, que incluem *smartphones, tablets* e *notebooks*".

A consumerização está vinculada à evolução em tecnologia da informação, aproximando o consumidor final de novas tendências em dispositivos móveis e, consequentemente, transportando estes equipamentos para as organizações onde trabalham e passam maior parte do tempo.

> A consumerização de TI alterou o cenário das inovações tecnológicas no decorrer dos anos, proporcionando uma situação na qual os consumidores possuem acesso às últimas tecnologias disponíveis, invertendo a lógica anterior, que dizia que a inovação chegava primeiramente aos ambientes corporativos. Neste mesmo contexto, a consumerização da TI mostra-se como grande motivadora da utilização de dispositivos pessoais para conectar-se a recursos corporativos (STAGLIANO, DIPOALO; COONELLY, 2013, p. 3).

O movimento de transposição do uso de dispositivos móveis pessoais para fins de trabalho é denominado de BYOD, tema que será tratado no próximo tópico.

1.2 BYOD

Por meio da consumerização, deu-se início ao fenômeno BYOD, do inglês "*Bring Your Own Device"*, ou, em tradução livre, "traga seu próprio dispositivo".

> Por BYOD entende-se a prática incorporada por algumas empresas de passar a permitir – dentro de uma política corporativa, organizada e alinhada à estratégia de negócio – que seus funcionários tragam os seus dispositivos pessoais, sejam eles *notebooks, smartphones, tablets* ou similares para o ambiente corporativo, com acesso à rede e aos sistemas da empresa (CERIONI, 2012, p. 4).

Segundo Moretti (2013, s/p), a utilização do BYOD tem como objetivo proporcionar maior liberdade aos funcionários diante de uma rotina de trabalho maçante, trazendo mais entusiasmo e motivação. Com isso, os trabalhadores acabam permanecendo em seus postos por mais tempo, muitas vezes sem questionar.

De acordo com pesquisa realizada pelo IBSG (2012, p. 6), o objetivo dos usuários ao levar dispositivos pessoais para o ambiente de trabalho é aproveitar os benefícios destas tecnologias para ganhar flexibilidade e produtividade. Dreibi (2012, s/p) complementa essa posição afirmando que os profissionais se sentem mais à vontade utilizando seus próprios equipamentos em detrimento dos fornecidos pelas empresas, pois estão mais familiarizados com eles.

A Intel Corporation (2012, p. 3) questionou 3.000 profissionais da área de tecnologia da informação e 1.300 usuários finais de BYOD sobre qual o principal uso dos dispositivos móveis no ambiente de trabalho, bem como qual era o equipamento utilizado para tanto. Os resultados podem ser observados na figura 2:

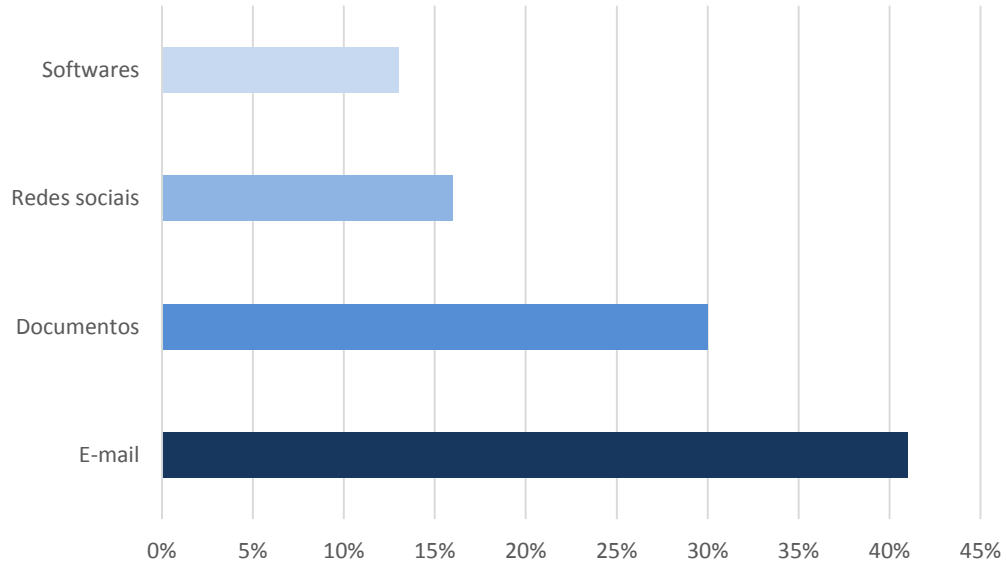
Figura 2 – Utilização do BYOD por profissionais de TI e usuários finais

	Estados Unidos			Alemanha			Austrália			Coréia do Sul		
Programas do pacote Office, como Word, Excel e PowerPoint	72%	77%	83%	65%	68%	74%	68%	77%	81%	83%	90%	92%
E-mails com arquivos e anexos	54%	49%	52%	46%	39%	39%	49%	41%	45%	46%	31%	35%
Calendário de datas corporativas	48%	45%	51%	46%	44%	49%	41%	38%	41%	33%	27%	28%
Lista de contatos e telefones úteis	41%	35%	42%	43%	35%	44%	37%	32%	38%	40%	35%	37%
Programas com controle de acesso	18%	9%	5%	20%	11%	8%	20%	11%	8%	24%	12%	7%
Sistemas de Gestão Empresarial (ERP)	11%	5%	2%	20%	11%	9%	12%	9%	8%	34%	13%	12%
Folha de pagamento e outros programas de Recursos Humanos	20%	7%	5%	19%	12%	8%	18%	10%	8%	34%	12%	10%

Fonte: Intel Corporation – Insights on the Current State of BYOD (2012, p. 6)

Já o estudo divulgado pela GovLoop (2013, p. 9) solicitou apenas a usuários finais que escolhessem, entre quatro alternativas, quais eram mais recorrentes na utilização de dispositivos móveis. As estatísticas encontram-se no gráfico 1:

Gráfico 1 – Utilização do BYOD por usuários finais



Fonte: elaborado pelo autor

Através da interpretação do gráfico acima (Gráfico 1), percebe-se que três dos quatros principais usos relacionam-se às atividades corporativas, de fato. O uso de redes sociais, entretanto, denota que a utilização do BYOD não está exclusivamente voltada para práticas organizacionais, ficando sob critério do usuário.

Cerioni (2012, p. 6) afirma que “o grande desafio para os diretores de tecnologia consiste em encontrar um equilíbrio entre a necessidade de controle e a liberdade concedida aos profissionais”. Tendo esta sentença como base, os subtópicos a seguir tratarão das vantagens e desvantagens obtidas pelo uso do BYOD, bem como os desafios envolvidos em sua utilização.

1.2.1 VANTAGENS

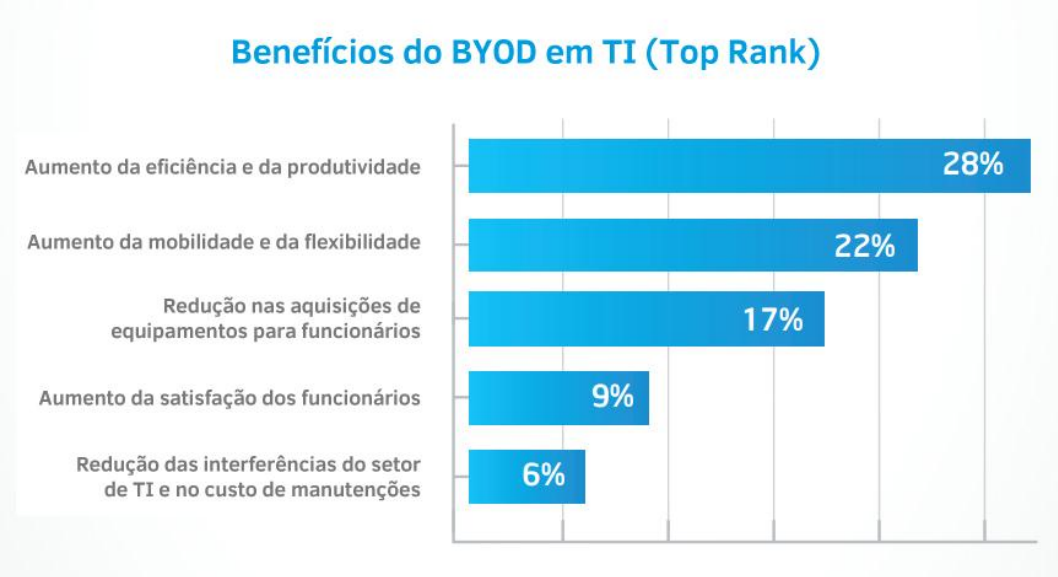
Permitir o uso de dispositivos móveis pessoais por funcionários no ambiente de trabalho pode ser vantajoso não apenas para a empresa, mas também para o colaborador. Segundo Wainwright (2012, s/p), pode-se listar seis aspectos positivos do BYOD:

- Satisfação dos funcionários: utilizar equipamentos com os quais já estão familiarizados, ao invés daqueles disponibilizados pela empresa, proporciona maior satisfação aos colaboradores;
- Dispositivos atualizados: a tecnologia está em constante mudança, tornando quase impossível às empresas manterem-se atualizadas com as novas tendências em equipamentos. Tendo em vista que o consumo pessoal de dispositivos se encontra em ritmo acelerado, as companhias podem se beneficiar de tecnologia de ponta através do BYOD;
- Redução de custos: com a implementação de um projeto de BYOD, as organizações podem transferir custos de conectividade e *upgrades* para os funcionários;
- Aumento de produtividade: permitir aos funcionários que utilizem dispositivos com os quais estão familiarizados aumenta a frequência e a velocidade de resposta às tarefas corporativas, acarretando um aumento significativo na produtividade organizacional;

- Redução de atribuições do departamento de T.I.: através do BYOD, os próprios funcionários tornam-se responsáveis pela manutenção de seus dispositivos, reduzindo as incumbências do setor de tecnologia da informação e permitindo que este concentre-se em questões de maior importância para a corporação.
- Comprometimento dos funcionários fora do ambiente de trabalho: a possibilidade de acessar informações da companhia em qualquer local e a qualquer momento faz com que os colaboradores continuem produzindo mesmo após o fim do expediente.

De acordo com a Intel Corporation (2012, p. 8), a utilização do BYOD também traz vantagens de menor expressão para as empresas, como a agilidade no recrutamento de novos funcionários, a redução no tempo de treinamento dos mesmos e a desaceleração no ciclo de renovação de equipamentos da empresa. As vantagens mais perceptíveis foram compiladas na imagem 3:

Figura 3 – Benefícios do BYOD em Tecnologia da Informação



Fonte: Intel Corporation – Insights on the Current State of BYOD (2012, p. 8)

Segundo Dreib (2012), os principais benefícios proporcionados às empresas pelo BYOD relacionam-se ao aspecto financeiro.

> Com cada funcionário utilizando seu dispositivo pessoal para o trabalho, há diminuição nos custos de manutenção do parque de máquinas, restando apenas o custo de manutenção das contas dos funcionários. O empregado também é beneficiado, pois além de

> desempenhar suas atividades com facilidade e rapidez, aumenta a produtividade contribuindo para o crescimento financeiro e geral da empresa (DREIB, 2012, s/p).

Apesar das muitas vantagens apresentadas, o BYOD também possui pontos negativos. Estes aspectos serão tratados no subtópico seguinte.

1.2.2 DESVANTAGENS

As vantagens da utilização do BYOD no ambiente de trabalho podem mascarar e até mesmo estar diretamente ligadas a aspectos negativos. De acordo com Matteucci (2017, s/p), as principais desvantagens do uso de dispositivos móveis na esfera corporativa são:

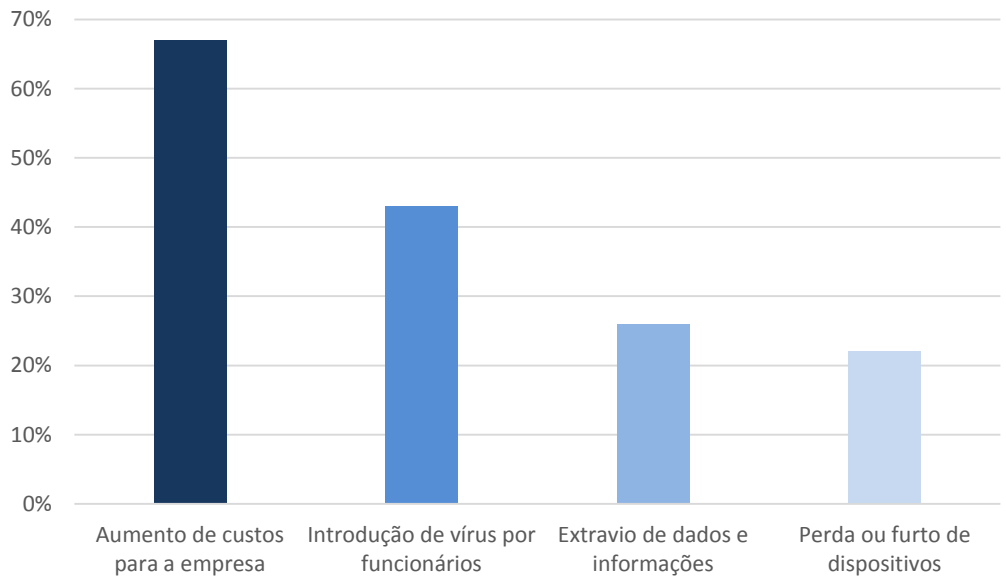
- Custos para os funcionários: a utilização de dispositivos pessoais reduz os encargos financeiros das empresas, redirecionando-os aos funcionários. Os colaboradores passam a arcar com a aquisição de equipamentos, com a manutenção dos mesmos e com serviços extras como conectividade remota, aplicativos licenciados e *updates*;
- Incompatibilidade de dispositivos: como os empregados tendem a investir em equipamentos cada vez mais novos, é possível que haja disparidade entre os dispositivos pessoais e os utilizados pela empresa, impedindo o funcionamento correto de programas e do compartilhamento de informações;
- Aumento de atribuições do departamento de T.I.: o aspecto da transferência de responsabilidade do setor de tecnologia da informação para o funcionário foi mencionado como uma vantagem anteriormente, mas também possui seu viés negativo. Os técnicos deixam de acompanhar o histórico de pendências dos dispositivos e acabam sendo acionados apenas quando já não há possibilidade de reparo, criando transtornos maiores do que seriam as manutenções periódicas nos equipamentos.
- Riscos legais: utilizar dispositivos pessoais para fins profissionais fora do ambiente corporativo pode trazer contratempos jurídicos para a empresa. Existem leis específicas para transferência internacional de informações, bem como para retenção e exclusão dos dados por parte dos colaboradores. O problema mais comum, entretanto, é a falta de um limiar bem delineado entre o que pode ser

considerado uso ocasional da força de trabalho fora do horário comercial e o que, de fato, deve-se tornar hora extra e remunerada.

- Perda, furto ou danos aos dispositivos: a flexibilidade ocasionada pelo BYOD em transpor os limites físicos da empresa traz consigo ameaças aos dispositivos portáteis. Seja por descuido dos colaboradores ou por ação de criminosos, é possível que os equipamentos sejam extraviados, colocando em risco todas as informações corporativas neles contidos.
- Aumento das falhas de segurança: este é, sem dúvida alguma, o ponto negativo **principal da utilização do BYOD. Por tratar-se de um tema abrangente, este assunto** será apresentado como tópico individual no desenvolvimento deste trabalho.

As desvantagens inerentes à utilização dos dispositivos pessoais fazem com que as empresas acabem proibindo a prática do BYOD. As principais razões para esta proibição foram relacionadas por uma pesquisa conduzida pela Lieberman Software Corporation (2012, s/p) junto a 250 profissionais de TI, como pode-se observar no gráfico 2:

Gráfico 2 – Motivações para proibição do BYOD



Fonte: elaborado pelo autor

Por meio do gráfico acima é possível perceber que esta pesquisa indica que, ao contrário do mencionado por Wainwright (2012, s/p), o BYOD gera aumento de custos para a empresa. Segundo Kumar (2014, s/p), dentre os fatores para elevação de encargos estão a remuneração de horas extras aos funcionários, o pagamento de indenizações trabalhistas decorrentes de práticas não regulamentadas do BYOD e a necessidade de contratar planos mais eficientes de conexão à internet, motivados pelo acesso à rede de mais dispositivos ao mesmo tempo.

Para que a utilização de dispositivos móveis no ambiente corporativo proporcione mais aspectos positivos do que desvantagens para a empresa, é necessário que a prática seja desenvolvida de maneira correta. Sendo assim, o próximo capítulo apresentará um protocolo de implementação elaborado com o objetivo de maximizar a eficiência do BYOD.

1.3 IMPLEMENTAÇÃO DO BYOD

Todos os processos implementados em uma empresa seguem o chamado “ciclo PDCA”. Este ciclo é utilizado para “controlar um processo, com as funções básicas de planejar, executar, verificar e atuar corretamente” (DEMING, 1990, p. 79). Entretanto, é necessário entender que o fenômeno BYOD enquadra-se em uma nova era de tendências corporativas, exigindo uma estrutura de implementação mais ampla e complexa. Este capítulo tem como objetivo apresentar os métodos utilizados atualmente para inserir o uso de dispositivos móveis nas corporações.

1.3.1 ETAPAS DE IMPLEMENTAÇÃO

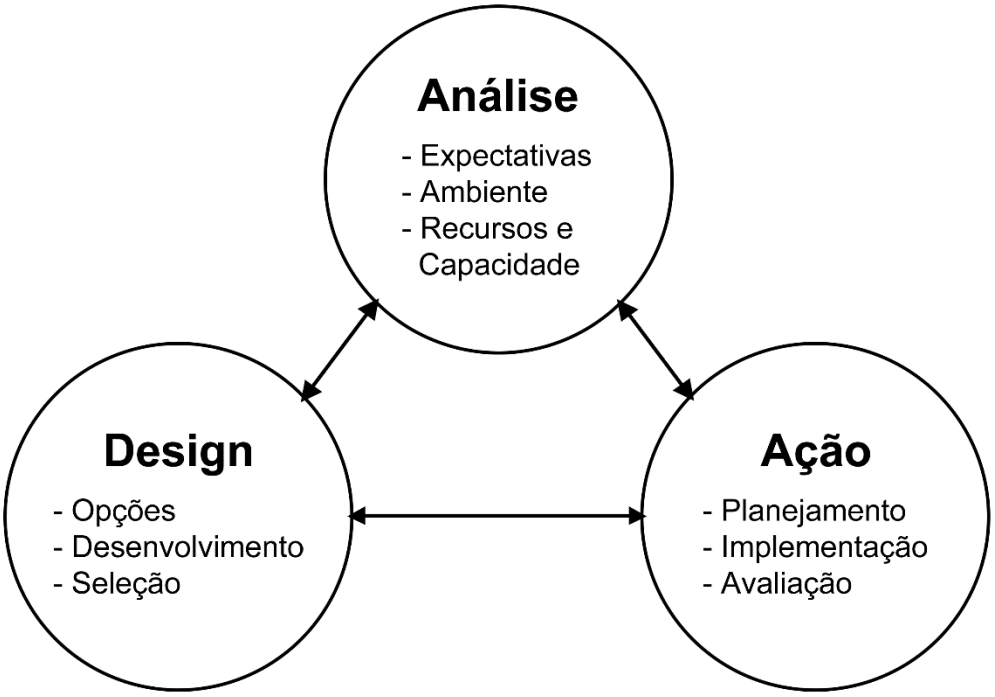
De acordo com Brodin (2015), utilizar um modelo de gerenciamento estratégico, em detrimento do modelo cíclico atual, proporciona uma visão mais clara do que deve ser feito para implementar o BYOD:

> Através da adaptação do modelo da série ISO 27000, diversas preocupações com segurança envolvidas no BYOD podem ser gerenciadas. Adotar o BYOD não representa, necessariamente, uma mudança na direção dos negócios de uma organização. Entretanto, haverá implicações no gerenciamento de informações estratégicas, motivo pelo qual o modelo sofreu modificações para se adaptar a este propósito. A estrutura principal deriva da proposição de Johnson

> e Scholes (1993), mas seu foco foi direcionado para a segurança da informação (BRODIN, 2015, p. 165).

A estrutura desenvolvida pelo autor pode ser observada na figura 4:

Figura 4: Estrutura proposta para implementação do BYOD



Fonte: Brodin (2015)

Como demonstrado na figura acima, as etapas para implementação do BYOD dividem-se em análise, design e ação, sendo que cada um dos passos possui atividades específicas. Todos estes tópicos serão tratados a seguir.

1.3.2 ANÁLISE

A fase de análise diz respeito às oportunidades e ameaças envolvidas na implementação do BYOD, incluindo as expectativas criadas com relação ao uso dos dispositivos móveis, como o ambiente corporativo será afetado e quais recursos e capacidades a organização possui para alcançar os benefícios ambicionados e mitigar possíveis efeitos negativos.

- Expectativas: os profissionais de TI esperam que a implementação do BYOD traga aumento de produtividade entre os colaboradores, flexibilidade de atuação em termos de tempo e espaço e, consequentemente, aumento de rendimentos para a empresa. A ameaça relacionada a este tópico reside no aumento do nível de *stress* dos colaboradores que, por trabalharem além do horário de expediente e das instalações físicas da empresa, podem acabar comprometendo sua qualidade de vida.

- Ambiente: este tópico da fase de análises relaciona-se quase que exclusivamente a ameaças. A prática do BYOD traz riscos iminentes à segurança da informação no ambiente corporativo, expondo as organizações a todo tipo de extravio de dados, além da inserção de elementos nocivos como vírus e *malwares*. Estes danos virtuais, por sua vez, podem acarretar em prejuízos pessoais, pois o uso mal regulamentado dos dispositivos móveis acaba por colocar em cheque a relação entre funcionários e gestores. O único aspecto positivo vislumbrado encontra-se justamente na oportunidade de evolução dos mecanismos de proteção da informação e na abertura de um diálogo franco entre colaboradores.

- Recursos e capacidade: averiguar qual a real habilidade da empresa em garantir que o BYOD traga mais benefícios que ameaças é a etapa final da fase de análise. Neste período deve-se reunir os dados obtidos nos tópicos anteriores para traçar o status atual da organização, a qual nível ela deseja chegar e quais são as ferramentas disponíveis para tanto. Tendo estas informações em mãos, procede-se à etapa de design, que começará a delinear quais as alternativas possíveis para implementar o BYOD.

1.3.3 DESIGN

A fase de design inicia-se com o desenvolvimento de estratégias nas áreas de gestão e informação, bem como de políticas para a utilização do BYOD. Nesta etapa, define-se as diferentes opções estratégicas possíveis, enumerando-as e realizando as adaptações necessárias para, por fim, escolher a mais adequada à empresa.

- Opções: as opções estratégicas possíveis para implementação do BYOD variam entre os extremos de proibir completamente o uso de dispositivos móveis e liberar a prática sem nenhum tipo de restrição. Nenhuma destas alternativas, entretanto, é recomendada por especialistas na área. Deve-se buscar um meio termo entre os interesses e as necessidades dos colaboradores e dos gestores, avaliando quando concessões ou vetos podem colocar a empresa em risco.
- Desenvolvimento: neste tópico da fase de design, deve-se enumerar as opções estratégicas apresentadas e desenvolver métodos para sanar as falhas averiguadas previamente. Raramente uma alternativa cobrirá todos os pontos de atenção considerados essenciais pela companhia, fazendo-se necessária a adaptação de políticas de acordo com a cultura organizacional.
- Seleção: após verificar os benefícios e riscos presentes em cada opção apresentada e fazer as modificações necessárias, deve-se selecionar qual alternativa será adotada. Essa seleção levará à próxima fase da implementação do BYOD, na qual serão tomadas ações concretas para sua inserção.

1.3.4 AÇÃO

A fase final da implementação do BYOD refere-se à operacionalização da estratégia selecionada para tanto. De todas as etapas apresentadas, esta é a que mais se assemelha ao processo de gerenciamento empregado atualmente, no qual planeja-se o melhor método para introduzir um novo processo e posteriormente avalia-se quais os resultados obtidos.

Nesta etapa do estudo, Brodin (2015) argumenta que o BYOD é um fenômeno relativamente recente, e poucos pesquisadores fazem referências claras e diretas à fase de ação.

> Ainda que não haja uma noção sólida sobre as ações necessárias para a implementação do BYOD, os autores do assunto concordam com uma palavra-chave envolvida nesta etapa: treinamento. É necessário focar no aspecto humano e informacional em detrimento à tecnologia, tendo em vista o surgimento desenfreado de novas tendências, mas o princípio imutável da interação humana. Manter-se atualizado com relação a novas práticas de segurança da informação e educar os usuários para que saibam interagir com tais é fundamental para o sucesso do BYOD nas organizações (BRODIN, 2015, p. 167).

Gatewood (2012, p. 30) compartilha desta opinião, afirmando que “o treinamento dos funcionários para a segurança da informação é de suma importância, pois os mecanismos técnicos de nada valem sem o comprometimento dos colaboradores.”

Ainda que os autores enfatizem a importância do elemento humano na prática do BYOD, é indiscutível que garantir a integridade das informações corporativas seja um ponto crítico na utilização de dispositivos móveis no ambiente organizacional. O próximo capítulo tratará do conceito e da gestão da segurança da informação, demonstrando quais ações podem ser adotadas para auxiliar neste processo.

2 SEGURANÇA DA INFORMAÇÃO

Com o surgimento de novas tecnologias e o crescente vínculo do funcionamento de corporações aos sistemas virtuais, as empresas viram-se expostas à novas ameaças e passaram a se preocupar com a segurança de suas informações.

> As redes de computadores, e consequentemente a Internet, mudaram as formas como se usam os sistemas de informação. As possibilidades e oportunidades de utilização são muito mais amplas que em sistemas fechados, assim como os riscos à privacidade e a integridade da informação. Portanto, é muito importante que mecanismos de segurança de sistemas de informação sejam projetados de maneira a prevenir acessos não autorizados aos recursos e dados destes sistemas (LAUREANO, 2005, p. 11).

Para melhor compreender as alternativas possíveis para garantir a segurança das informações, faz-se necessário conceituar o tema e definir os pontos de prioridade para sua gestão.

2.1 CONCEITO

De acordo com Fontes (2008, p. 114), a segurança da informação pode ser definida como “um conjunto de orientações, normas, procedimentos, políticas e demais ações que tem como objetivo proteger o recurso da informação”. Por informação entende-se um “conjunto de dados, ao qual se atribui valor, utilidade ou interpretação, que pode representar um grande diferencial para seus detentores” (COSTA NOVO, 2010, p. 27).

Em um conceito mais abrangente, Dias (2000, p. 48) argumenta que a segurança da informação é a proteção dos sistemas informação contra a inserção, modificação e exclusão de dados, armazenados, em processamento ou já compilados, por usuários não autorizados. A segurança da informação deve abranger a segurança dos recursos humanos, dos documentos, das áreas e das instalações computacionais e de comunicação, assim como deve prevenir, detectar, prever e reportar eventuais ameaças (WADLOW, 2000, p. 125).

> É necessário compreender que a segurança da informação possui papel primordial em uma organização, pois a informação, em si, é muito mais do que apenas um conjunto de dados. A informação, quando utilizada de maneira estratégica, transforma algo com pouco

> significado em um recurso de valor incalculável para a empresa (FONTES, 2008, p. 131).

Ainda que as corporações devam analisar qual mecanismo é mais conveniente para o funcionamento e o cumprimento de suas políticas, alguns requisitos devem ser necessariamente atendidos para garantira segurança da informação, como será explanado a seguir.

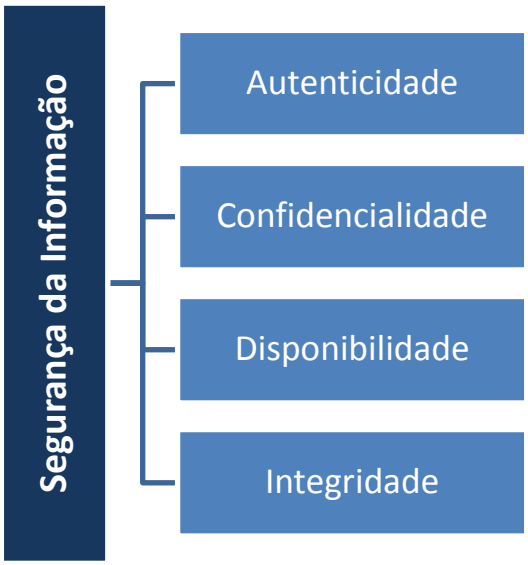
2.2 GESTÃO DA SEGURANÇA

Diferentes setores organizacionais possuem diferente tipos de gestão, não sendo diferente com a segurança da informação. Ferreira e Araújo (2008, pp. 44-47) destacam quatro pontos de atenção para uma administração eficiente nesta área: integridade, confidencialidade, disponibilidade e autenticidade.

- Autenticidade: é o aspecto que garante a proteção no envio de informações, assegurando que não haja modificações durante a transmissão ao remetente.
- Confidencialidade: a informação só pode ser acessada por pessoas autorizadas, sendo definidos níveis de hierarquia e prioridade. A identificação do usuário que está acessando a informação é parte fundamental deste aspecto, pois impede a exposição e a transmissão inadequada dos dados.
- Disponibilidade: é a garantia de que as informações estarão disponíveis de modo fácil e confiável para usuários autorizados.
- Integridade: as informações devem ser armazenadas em seu formato original, assegurando que qualquer modificação ou exclusão de dados sem autorização não comprometa as características inicias da informação.

Os requisitos listados podem ser representados de acordo com a figura 5:

Figura 5: Requisitos básicos da segurança da informação: princípios originais



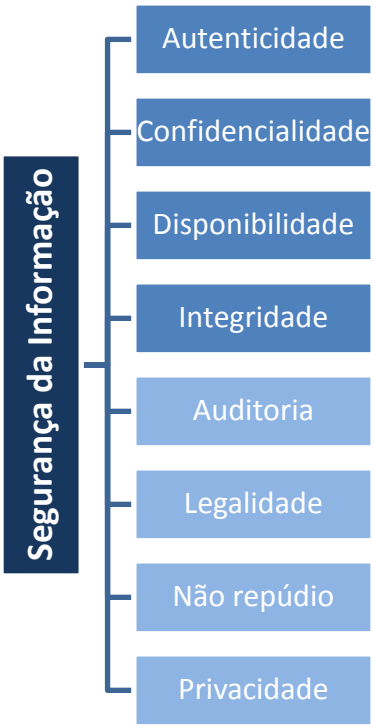
Fonte: elaborado pelo autor

Com a evolução da segurança da informação, alguns autores adicionaram novos requisitos a serem cumpridos para abranger ainda mais a proteção dos dados. De acordo com Sêmola (2014, p. 112), para ser eficiente a gestão da segurança da informação deve atender, além dos princípios originais, os seguintes aspectos:

- Auditoria: deve ser possível monitorar e reportar os diversos processos aos quais as informações são submetidas, identificando usuários, locais, datas e horários de cada etapa. Manter uma auditoria eficiente possibilita identificar violações de segurança;
- Legalidade: é o aspecto jurídico da informação, que deve estar em acordo com as legislações políticas, institucionais, nacionais e internacionais vigentes. Se as informações não respeitarem tais códigos, não terão valor legal;
- Não repúdio: não se deve negar ou omitir a recepção, modificação ou envio das informações, bem como qual operação, serviço ou usuário a executou;
- Privacidade: este princípio difere da confidencialidade pois, por se tratar de uma informação privada, o usuário não deve ser identificado. Não é recomendado que dados particulares sejam armazenados em uma rede corporativa, mas caso seja necessário, deve-se garantir que o indivíduo que acessá-los não seja rastreado.

Os princípios formulados recentemente, quando incorporados aos originais, podem ser observados na figura 6:

Figura 6: Requisitos básicos da segurança da informação: novos princípios



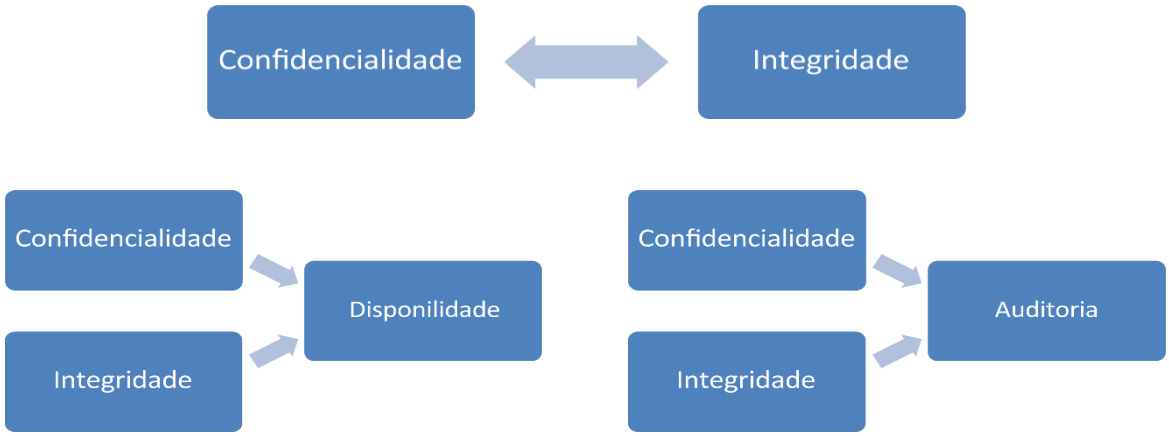
Fonte: elaborado pelo autor

Além da apresentação dos requisitos básicos, Stoneburner (2015, p. 3) ainda traça uma relação entre eles. O autor afirma que a confidencialidade depende da integridade, pois se esta for perdida, os mecanismos que controlam a confidencialidade não são mais válidos. Por outro lado, a integridade também é dependente da confidencialidade, já que se alguma informação sigilosa for comprometida, os dispositivos de integridade podem ser desativados.

A auditoria e a disponibilidade também são dependentes dos aspectos de confidencialidade e integridade, pois perde-se o propósito em registrar o histórico de alterações e em manter as informações disponíveis caso elas deixem de ser confiáveis e sigilosas.

Todas estas relações ficam ilustradas de maneira simplificada na figura 7:

Figura 7: Relação entre os requisitos da segurança da informação.



Fonte: elaborado pelo autor

Além dos requisitos básicos que devem ser atendidos para uma gestão de segurança da informação eficiente, existem determinados procedimentos que operam de acordo com estes princípios e que devem ser adotados pelas organizações de acordo com suas normas internas. O capítulo a seguir tratará de políticas gerais e específicas aplicadas para garantir a segurança da informação no meio corporativo.

2.3 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

De acordo com Fontes (2008, p. 154), as políticas de segurança da informação “são mecanismos que garantem a viabilidade e o uso das informações somente por pessoas autorizadas”. Estas políticas devem ser comunicadas a todos os funcionários e requerem análise e revisão constante, em intervalos regulares ou sempre que necessário.

> A política tende a estabelecer regras e normas de conduta com o objetivo de diminuir a probabilidade da ocorrência de incidentes que provoquem, por exemplo, a indisponibilidade do serviço, furto ou até mesmo a perda de informações. Normalmente são construídas a partir das necessidades do negócio e eventualmente aperfeiçoadas pela experiência do gestor (DANTAS, 2011, p. 133).

As políticas de segurança da informação devem ser desenvolvidas, modificadas e adotadas de acordo com a necessidade das organizações. Entretanto, existem métodos gerais e específicos que vêm se mostrando eficientes ao longo de suas aplicações. Tais métodos serão apresentados a seguir.

2.3.1 POLÍTICAS GERAIS

As políticas de segurança gerais são aquelas que norteiam o desenvolvimento de todas as outras. Tratam-se de roteiros de boas práticas para auxílio à gestão da segurança da informação e foram estruturados por organizações de TI conhecidas e respeitas em todo o mundo.

2.3.1.1 ISO 27001

A norma ISO 27001 é um padrão para políticas de segurança da informação desenvolvido pela *International Organization for Standardizatione* pela *International Electrotechnical* Comission, e publicado pela primeira vez em 2005. “Esta norma foi elaborada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar os sistemas de segurança da informação” (ISO 27001, 2015, s/p).

A ISO 27001 pertence à ISO 27000, uma série de padrões de certificação relacionados à gestão da segurança da informação. A versão mais recente da ISO 27001 foi publicada em 2013.

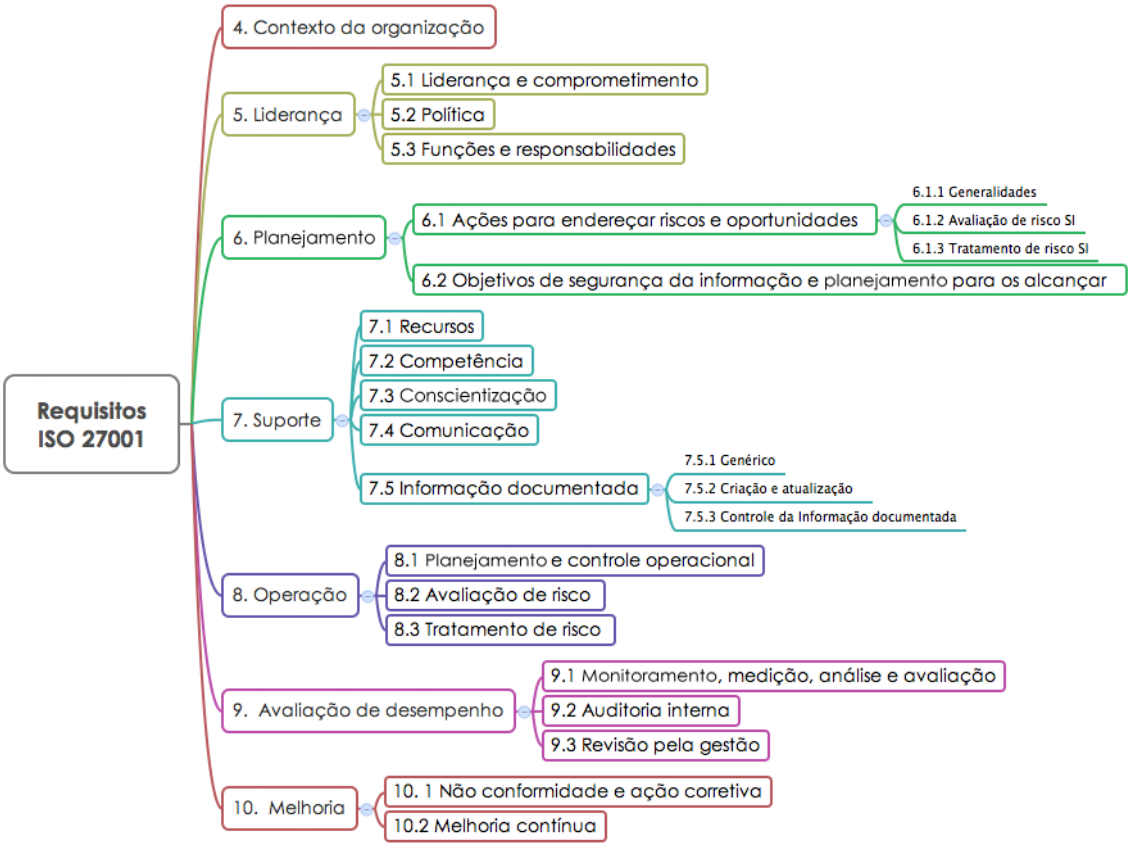
> A ISO 27001 pode ser implementada em qualquer tipo de organização, com ou sem fins lucrativos, privada ou pública, pequena ou grande. Ela é escrita pelos melhores especialistas mundiais no campo de TI e provê metodologia para a implementação de políticas de segurança da informação em uma organização. Ela também possibilita às empresas a obtenção de certificado, o que significa que estão em conformidade com os padrões instituídos pela ISO (ADVISERA, 2017, s/p).

O foco da ISO 27001 é proteger os requisitos básicos da gestão da segurança da informação, ou seja, confidencialidade, integridade, disponibilidade e autenticidade. De acordo com a Advisera (2017), isto é feito por meio da identificação de quais problemas em potencial podem ocorrer à informação e pela

definição de quais necessidades devem ser atendidas para prevenção de tais problemas.

Segundo a Integrity Consulting & Advisory (2017, s/p), a certificação ISO 27001 é composta por duas etapas. A primeira etapa consiste em definir as regras e requisitos do cumprimento da norma, como demonstrado na figura 9:

Figura 9: Primeira etapa da certificação ISO 27001



Fonte: Integrity Consulting &Advisory – ISO 27001: em que consiste? (2017, s/p)

Já a segunda etapa é denominada de Anexo A e é composta por um conjunto de controles que devem ser adotados pela organização, em diferentes áreas:

Figura 10: Segunda etapa da certificação ISO 27001

Fonte: Integrity Consulting & Advisory (2017, s/p)

De acordo com Kosutic (2010), após as duas etapas iniciais da certificação, começa a fase de auditoria. Neste período, um auditor visitará a empresa para verificar se os procedimentos constantes na documentação apresentada estão realmente sendo seguidos. Caso a empresa seja bem-sucedida nesta etapa, a certificação ISO lhe é concedida e possuirá validade de três anos, podendo ser revogada caso sejam encontradas irregularidades em nova visita do auditor.

Por meio da análise dos requisitos propostos pela ITIL e pela ISO 27001, pode-se ter uma base para formular políticas de segurança ainda mais particulares para as organizações, tendo em vista que as duas certificações mencionadas tratam-se de guias comportamentais e técnicos para implementar ações concretas.

No capítulo a seguir serão apresentadas políticas de segurança da informação específicas para companhias que pretendem implementar o uso do BYOD, pois contam com mecanismos de proteção compatíveis com a utilização dos dispositivos móveis em questão.

2.4 POLÍTICAS ESPECÍFICAS PARA BYOD

As políticas de segurança específicas para BYOD indicadas neste tópico têm como foco o controle de acesso às redes corporativas, o gerenciamento remoto de dispositivos móveis e a identificação e autenticação dos indivíduos que utilizarão tais equipamentos.

Assim como as políticas gerais, as específicas também devem ser adaptadas de acordo com o negócio ao qual serão aplicadas, de maneira a abranger ainda mais possíveis falhas de segurança.

2.4.1 NAC

A política de NAC, do inglês "*Network Access Control*" ou "Controle de Acesso à Rede", em tradução livre, foi criada em 2003 pela empresa Cisco, multinacional especializada em TI e sediada na Califórnia, Estados Unidos. Trata-se de um método utilizado para garantir que apenas dispositivos autorizados possam acessar a rede corporativa e de que eles terão que se identificar antes de realizar o acesso (BLACKBOX, 2010, p. 2).

De acordo com Garanhani (2013, p.23), o NAC são basicamente ferramentas que asseguram o controle de acesso a todos os dispositivos que, direta ou indiretamente, acessam a rede.

> Implementações do NAC bem arquitetadas por gerenciar facilmente diferentes níveis de usuário como, por exemplo, usuários confiáveis, que fazem parte de um determinado grupo de rede corporativa de uma empresa, e usuários convidados, pessoas ou determinados dispositivos externos que eventualmente conectam-se à rede. Este controle é baseado em critérios como identificação do usuário, tipo ou estado do dispositivo, dia e hora do acesso e departamento. Uma arquitetura NAC combinada a critérios de políticas bem segmentados torna o sistema de segurança mais robusto e alinhado com as necessidades do negócio (GARANHANI, 2013, p. 24).

O mapeamento de IP, tipo, sistemas operacionais e usuários dos dispositivos realizado pela política NAC está demonstrado na figura 11.

Figura 11: Tela extraída de um *software* de NAC

MAC Adress	Mobile Device Type	Operating System	Owner
90-21-55-EF-DD-9E	HTC EVO	Android 2.2	Chris
00-23-76-CD-C9-FB	HTC Hero	Android 2.3	Mike
40-FC-89-D2-2D-21	Droid Pro	Android 2.2.1	Tanya
3C-8B-FE-73-FE-9D	Samsung Galaxy Tablet	Android 2.2	IT
5C-DA-D4-50-99-1E	Samsung SCH-I500	Android 2.1	Joel
BC-47-60-B4-ED-FF	Samsung Intercept	Android 2.1	Andre
DC-2B-61-EA-38-47	iPhone	iOS 9	Jamie
F4-0B-93-66-88-33	Blackberry Bolt 9700	Blackberry	Tanya
00-25-AE-22-93-33	Zune HD	Windows CE	Riley

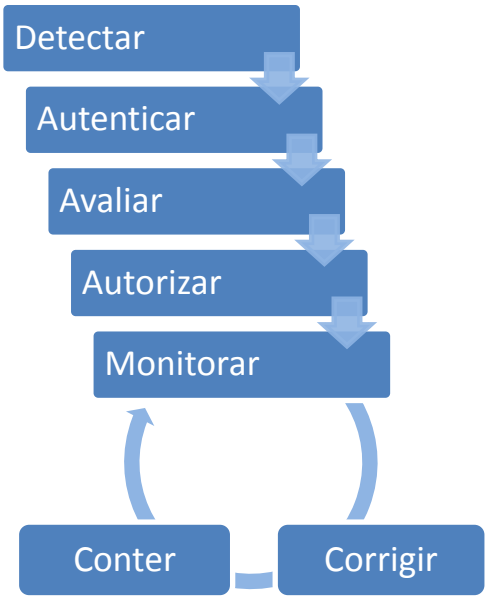
Fonte: Enterasys (2008, p. 18)

Segundo a empresa de segurança Enterasys (2008, p. 4), as funções da política NAC são:

- Detecção: identificar novos dispositivos que estejam solicitando conexão à rede corporativa;
- Autenticação: autenticar os usuários e dispositivos;
- Avaliação: analisar as conformidades e vulnerabilidades dos usuários e dispositivos;
- Autorização: permitir o uso da rede com base nos resultados da autenticação e da avaliação;
- Monitoramento: supervisionar os usuários e dispositivos enquanto estiverem utilizando a rede;
- Contenção: impedir que os usuários e dispositivos tenham impacto negativo na rede e em todo o ambiente corporativo;
- Correção: reparar possíveis danos que possam ter evadido as etapas anteriores.

A figura 12 demonstra a ordem de aplicação destas funções, ressaltando que as três últimas etapas, Monitoramento, Contenção e Correção, são cíclicas e constantes.

Figura 12: Estrutura de funções do NAC



Fonte: elaborado pelo autor

De acordo com a Cisco (2010), existem diferentes tipos de NACs; entretanto, o mais adequado para a prática do BYOD é o método que utiliza VRFs (*Virtual Routingand Forwarding)*. Os VRFs são componentes virtuais que seccionam a rede corporativa, criando diferentes níveis de acesso e encaminhando os usuários para áreas específicas da rede.

> Os VRFs coexistem na mesma estrutura física da rede corporativa, mas cada VRF cria uma rede virtual isolada para um grupo particular de usuários ou dispositivos. De acordo com a movimentação dos indivíduos pela *network*, o NAC assegura-se que os direitos de acesso e as medidas de segurança corretas sejam aplicadas a eles (CISCO, 2010, s/p).

Ainda que dispensando a linguagem técnica envolvida no NAC, pode-se compreender sua importância no controle do acesso de dispositivos móveis à rede corporativa. Entretanto, as soluções oferecidas por essa política abrangem apenas parcialmente as práticas envolvidas no BYOD, pois impedem o acesso não autorizado à *network*, mas não controlam as informações armazenadas no dispositivo após a utilização. Para tanto, deverá ser utilizada a política de MDM, apresentada no tópico a seguir.

2.4.2 MDM

O MDM, do inglês “*Mobile Device Management*” ou “Gerenciamento de Dispositivos Móveis”, em tradução livre, constitui-se em “uma política integrada e centralizada que permite administrar toda a base de dispositivos móveis das empresas” (MDM Solutions, 2017, s/p).

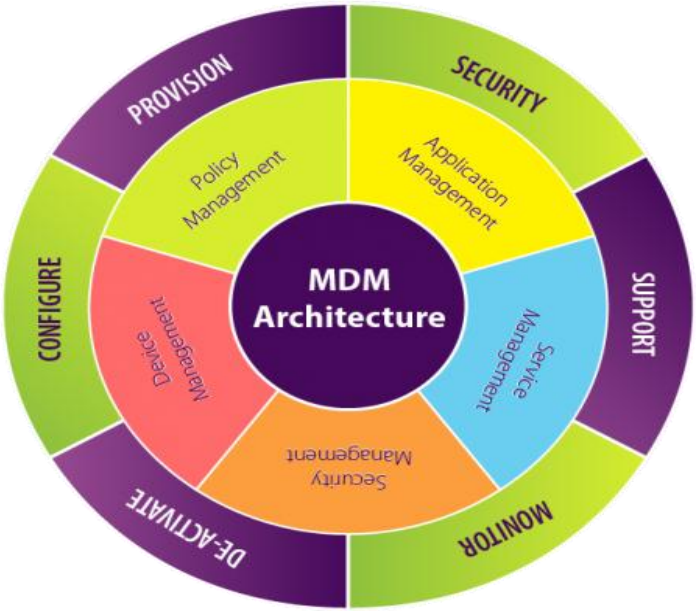
O principal objetivo do MDM é otimizar as funcionalidades e a segurança dos dispositivos móveis, simultaneamente protegendo a rede corporativa. Segundo a TechTarget (2013, s/p), os *softwares* de MDM permitem que os profissionais de TI gerenciem dispositivos móveis tão facilmente quanto dispositivos fixos, como *desktops*, monitorando quais áreas estão sendo acessadas pelos usuários.

De acordo com o XCubeLabs (2012, s/p), as principais funcionalidades do MDM podem ser listadas como:

- Configuração: ajusta o dispositivo de acordo com as normas da organização;
- Fornecimento: abastece os dispositivos com *softwares* corporativos e outros programas utilizados pela empresa;
- Segurança: protege a rede corporativa através de medidas de autenticação e acesso, bloqueando ou desbloqueando aplicativos e outras funcionalidades;
- Suporte: auxilia os usuários com problemas de TI em geral;
- Monitoramento: supervisiona o que está sendo realizado no dispositivo;
- Desativação: desliga e/ou inutiliza o dispositivo móvel remotamente.

A figura 13 demonstra a arquitetura do MDM, também considerando como funcionalidades o gerenciamento de serviços, políticas, aplicativos e segurança dos dispositivos.

Figura 13: Arquitetura de funcionalidades do MDM



Fonte: XCubeLabs – MDM: Enable, Manageand Secure your mobile environment (2012, s/p)

A principal diferença entre o MDM e o NAC é que este ocupa-se principalmente do controle de acesso de usuários à rede corporativa, enquanto que o outro foca nas informações armazenadas nos dispositivos móveis que realizam tal acesso. Para Madden (2011), a principal desvantagem do MDM é que esta política pode ser considerada invasiva pelos colaboradores, pois requer instalação nos equipamentos que serão monitorados, diferentemente do NAC.

> Muitas empresas que permitem a prática do BYOD solicitam a inspeção dos dispositivos de seus funcionários, recolhendo-os e instalando *softwares* de MDM, na maioria das vezes sem o consentimento dos proprietários dos aparelhos. Os programas de gerenciamento criam senhas de acesso, bloqueiam certas funcionalidades do aparelho e até mesmo apagam aplicativos como jogos e redes sociais (MADDEN, 2011, s/p).

Como pode-se observar após a análise das políticas gerais e específicas de segurança da informação, é indispensável que as organizações adotem normas, sejam técnicas ou de conduta, para que a utilização do BYOD não comprometa as informações corporativas.

Todas as referências apresentadas até agora apontam para o inevitável crescimento do uso de dispositivos móveis no ambiente organizacional. Por meio de uma implementação executada corretamente e o desenvolvimento de políticas de

segurança adequadas à empresa e aos usuários desta tecnologia, o BYOD tende a proporcionar mais vantagens do que pontos negativos para as empresas.

O próximo capitulo deste trabalho, apresentado a seguir, baseou-se na aplicação de um questionário à usuário potenciais e ativos do BYOD, objetivando conhecer, de maneira mais prática que teórica, o comportamento destes indivíduos em relação aos dispositivos móveis.

3 PESQUISA QUANTITATIVA

A pesquisa quantitativa desenvolvida para este estudo baseou-se em um questionário sobre o uso de dispositivos móveis pessoais no ambiente corporativo. As perguntas foram compiladas e estruturadas por meio da plataforma Google Forms, que possibilita a criação de formulários dinâmicos e descomplicados, facilmente acessíveis ao público.

O questionário é composto por treze perguntas e foi respondido por 43 indivíduos, usuários ou não da tecnologia BYOD, nos dias 24 e 25 de outubro de 2017. O formulário pode ser acessado através do endereço eletrônico <https://goo.gl/forms/dFrbYE3wOCMrvylr2>.

O objetivo desta pesquisa quantitativa foi traçar um perfil dos usuários efetivos do BYOD, identificando quais dispositivos são utilizados, com que frequência e para quais fins. Os indivíduos também foram questionados a respeito das políticas de segurança da empresa e quais pontos acreditam ser influenciados, positiva e negativamente, pelo uso dos dispositivos móveis pessoais.

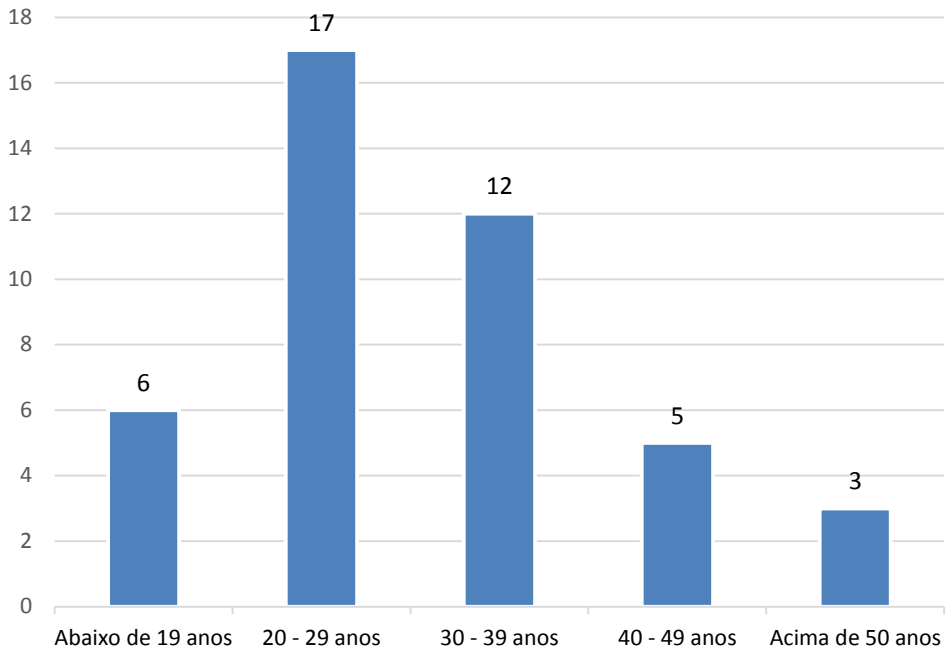
Com relação aos inquiridos que ainda não utilizam o BYOD, indagou-se se gostariam de fazer uso da tecnologia futuramente, de modo a confirmar a expansão da tendência verificada através da pesquisa bibliográfica.

Considerando que a pesquisa foi elaborada exclusivamente para este trabalho, dispensou-se a indicação de fonte nas legendas dos gráficos. Para propósitos de compreensão, a escala adotada será absoluta, ou seja, os resultados são expressos em número de participantes, e não pela porcentagem dos mesmos.

3.1 ANÁLISE DO QUESTIONÁRIO

A primeira pergunta do questionário trata-se de uma averiguação de idade, de modo a compreender em quais faixas etárias enquadram-se os indivíduos que participaram da pesquisa.

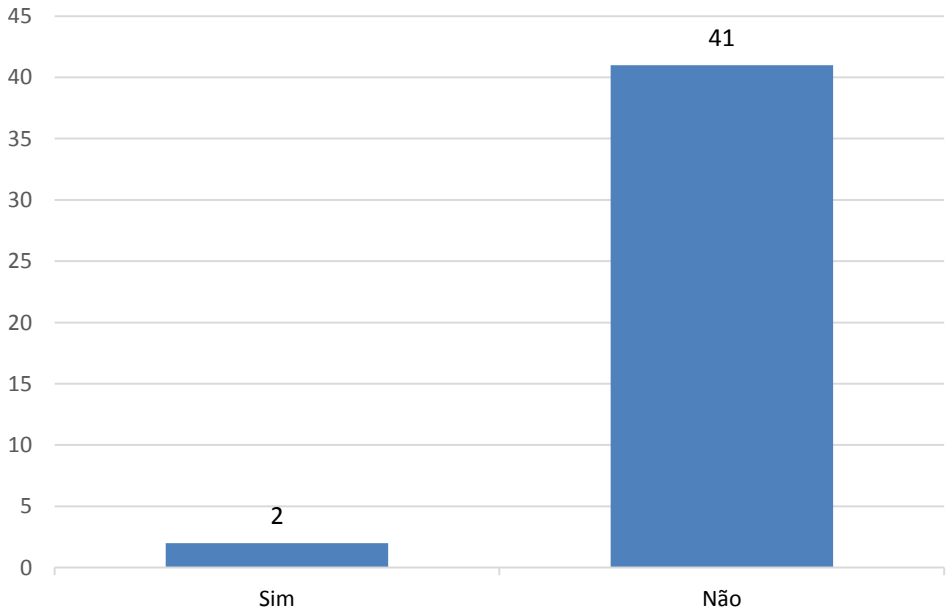
Gráfico 3 – Faixa etária dos participantes



Como demonstrado no gráfico 3, a maioria dos participantes possui entre 20 e 29 anos de idade, seguidos pela faixa etária de 30 a 39 anos e abaixo de 19 anos. Os dois menores grupos possuem entre 40 e 49 anos de idade ou estão acima dos 50 anos, consecutivamente.

Após a verificação de idade, questionou-se os participantes acerca do conhecimento do termo BYOD.

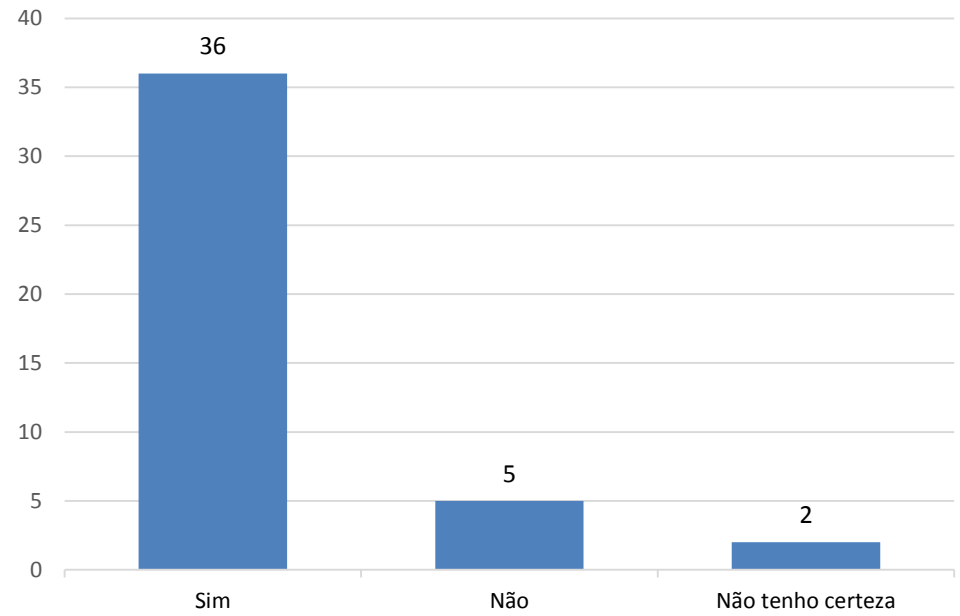
Gráfico 4 – Conhecimento do termo BYOD



Por meio do gráfico 4, percebe-se que pouquíssimas pessoas conhecem a expressão BYOD, sendo que apenas dois participantes da pesquisa identificaram o termo.

A terceira pergunta da pesquisa questionou se a empresa na qual os participantes atuam permite a prática do BYOD.

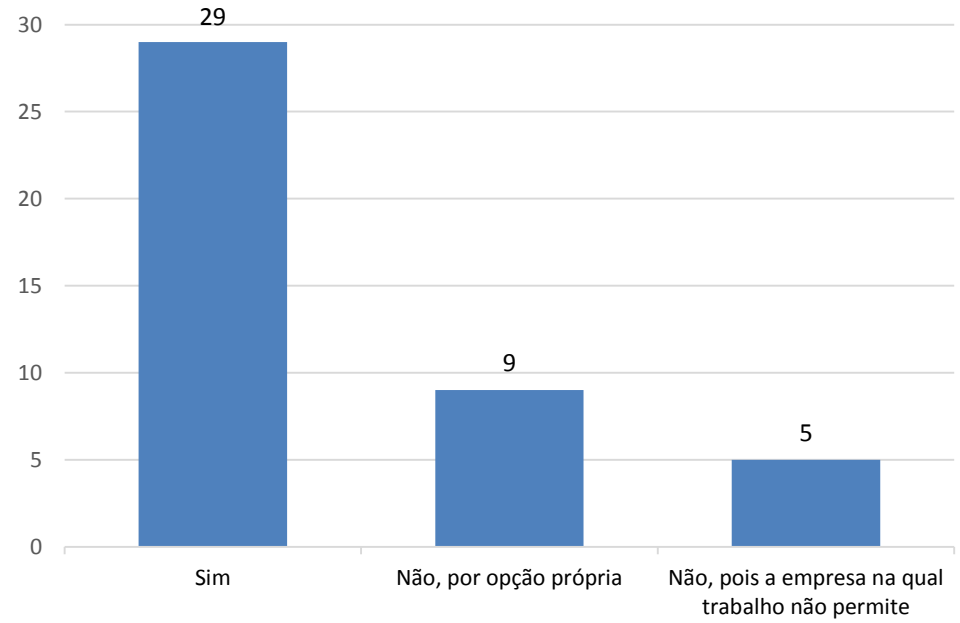
Gráfico 5 – Permissão do BYOD nas empresas



O gráfico 5 demonstra que a maioria das empresas nas quais os entrevistados atuam permite o uso de dispositivos móveis pessoais, estatística que corrobora os dados apresentados por Borrett (2013, pp. 5-6) e pelo IBSG (2012, p. 2).

Ainda que as organizações permitam a prática do BYOD, faz-se necessário saber se os seus colaboradores, de fato, utilizam os dispositivos móveis.

Gráfico 6 – Utilização efetiva do BYOD

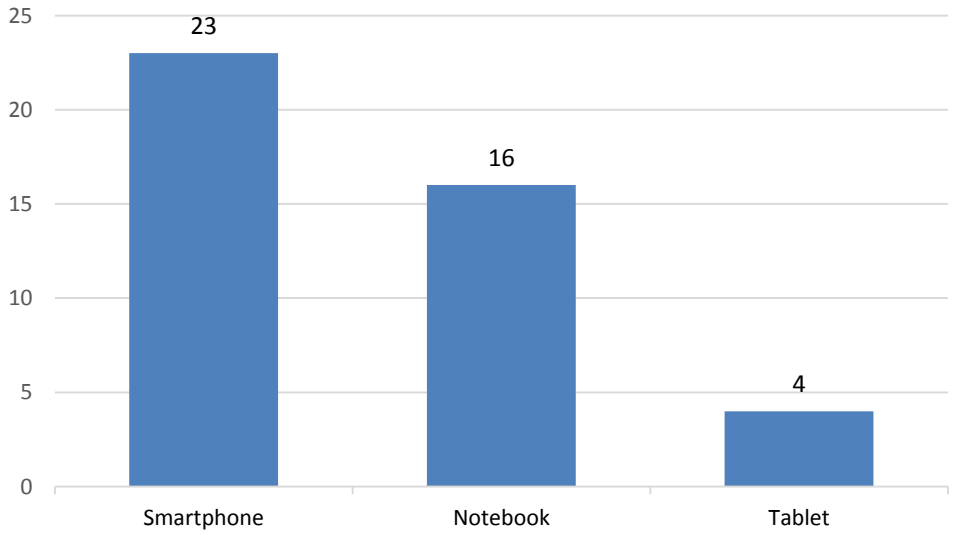


Como verificado através do gráfico 6, alguns participantes decidiram não utilizar seus dispositivos móveis pessoais para atividades corporativas, mesmo atuando em empresas que permitem a prática. A relação entre este e o quarto gráficos demonstra que os indivíduos fazem uso do BYOD mesmo desconhecendo a denominação apropriada para a prática.

A próxima etapa do questionário foi direcionada para usuários efetivos do BYOD. Os participantes que não utilizam dispositivos móveis foram orientados a avançar diretamente para a fase seguinte do formulário.

A quinta pergunta da pesquisa verificou qual o tipo de dispositivo móvel mais utilizado para atividades corporativas.

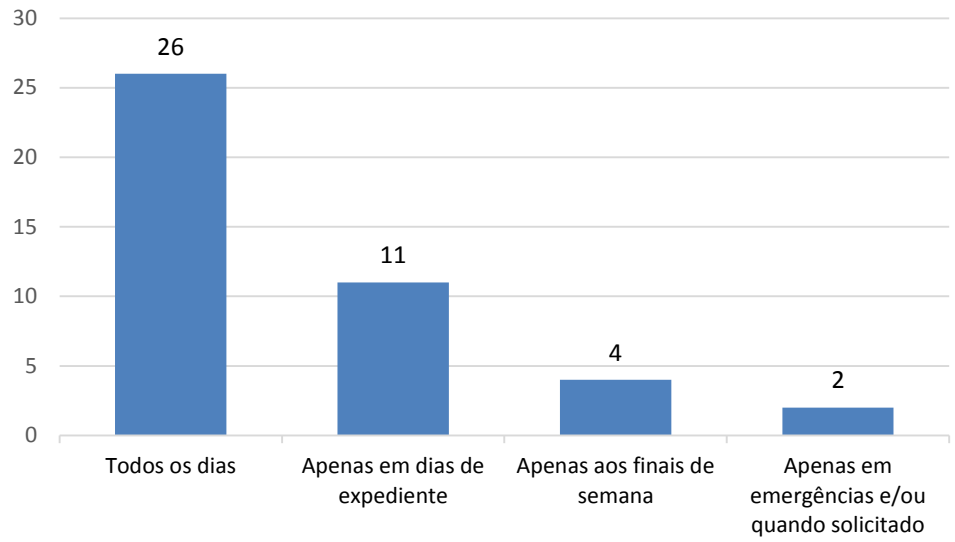
Gráfico 7 – Tipos de dispositivos móveis utilizados no BYOD



O gráfico 7 demonstra que os dispositivos móveis pessoais mais utilizados para fins profissionais são os smartphones, seguidos pelos notebooks e pelos tablets. Estes resultados confirmam os dados divulgados pela Fundação Getúlio Vargas (2017, p. 7).

Tendo identificado qual o equipamento utilizado, a próxima pergunta averiguou com que frequência é realizado este uso.

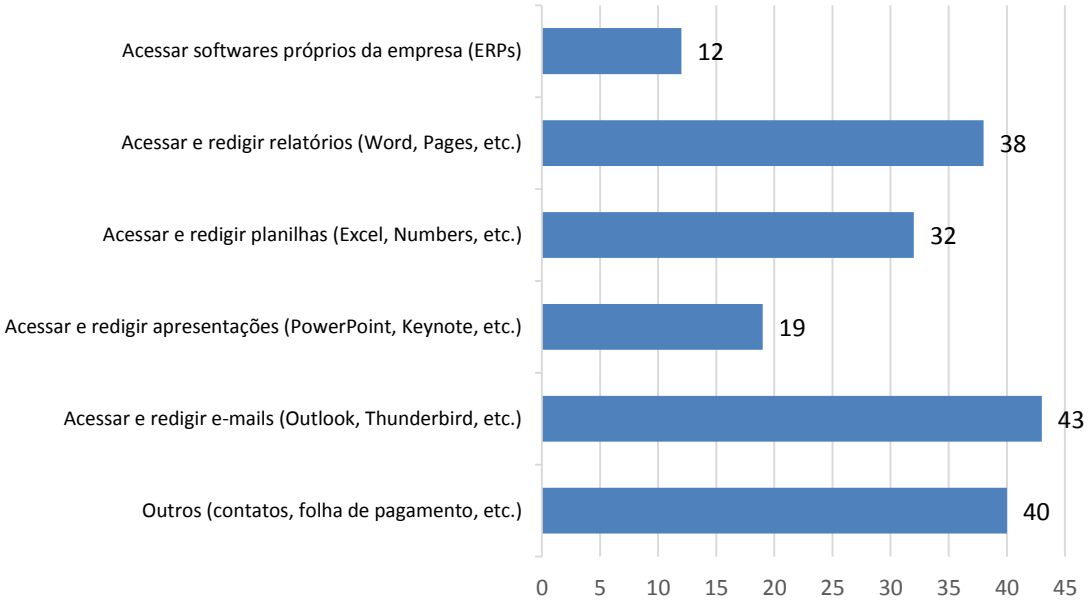
Gráfico 8 – Frequência de utilização dos dispositivos móveis



Como verificado no gráfico, a maioria dos participantes utiliza os dispositivos móveis diariamente. A menor parcela da pesquisa respondeu que só faz uso dos equipamentos diante de emergências ou quando solicitado.

Após responderem sobre a frequência de uso, os participantes foram indagados a respeito da finalidade da utilização, podendo escolher quantas alternativas fossem necessárias.

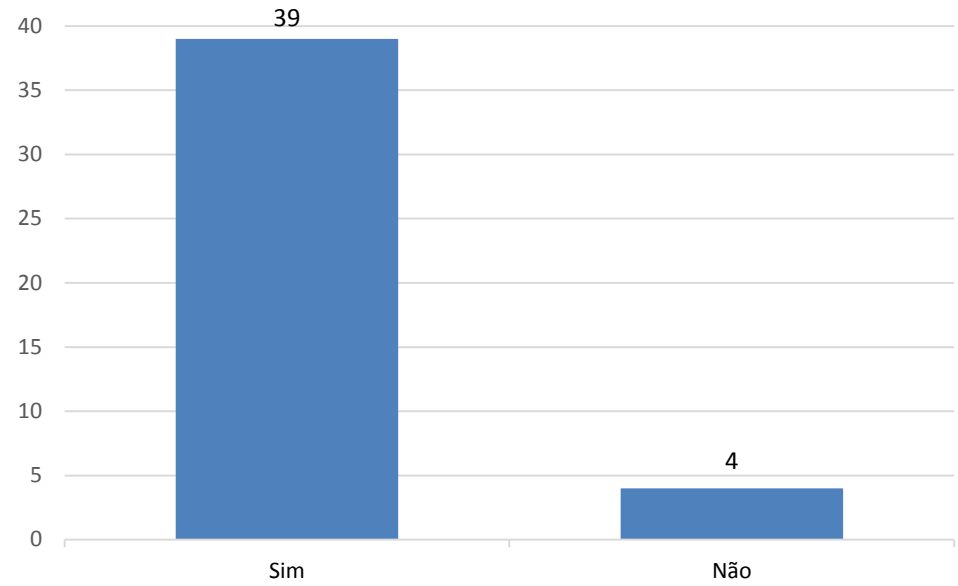
Gráfico 9 – Finalidade de utilização dos dispositivos móveis



O gráfico 9 demonstra que a principal finalidade do BYOD é o acesso a e-mails, seguido de funcionalidades básicas como lista de contatos, folha de pagamento, entre outros. A utilização de *softwares* para acessar e elaborar textos, planilhas e apresentações também teve adesão expressiva. O uso de programas próprios das organizações, os ERPs (Enterprise Resource Planning), foi a alternativa menos escolhida entre os participantes. Estas respostas ratificam a pesquisa realizada pela empresa GovLoop (2013, p. 9).

As próximas três perguntas do questionário dizem respeito às políticas de segurança da informação adotadas pelas empresas nas quais os participantes atuam. A primeira delas questionou sobre a existência de usuário e senha individuais para acesso às informações.

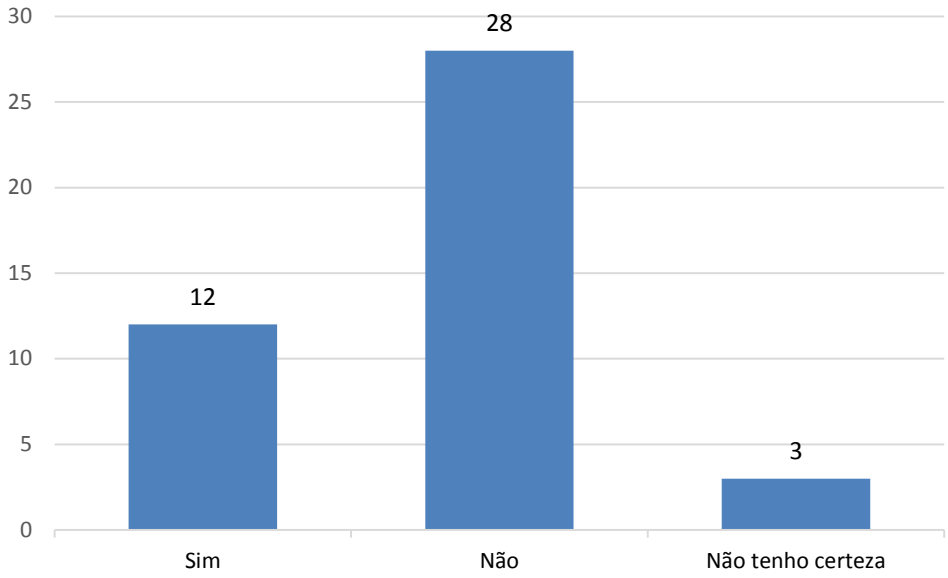
Gráfico 10 – Existência de acesso autenticado às informações corporativas



O gráfico 10 indica que a maioria das empresas exige usuário e senha personalizados para cada colaborador. Ainda assim, quatro participantes disseram que utilizam uma autenticação genérica para acessar as informações corporativas.

A nona pergunta averiguou se os usuários conhecem as políticas de segurança da informação adotadas pela empresa em que trabalham.

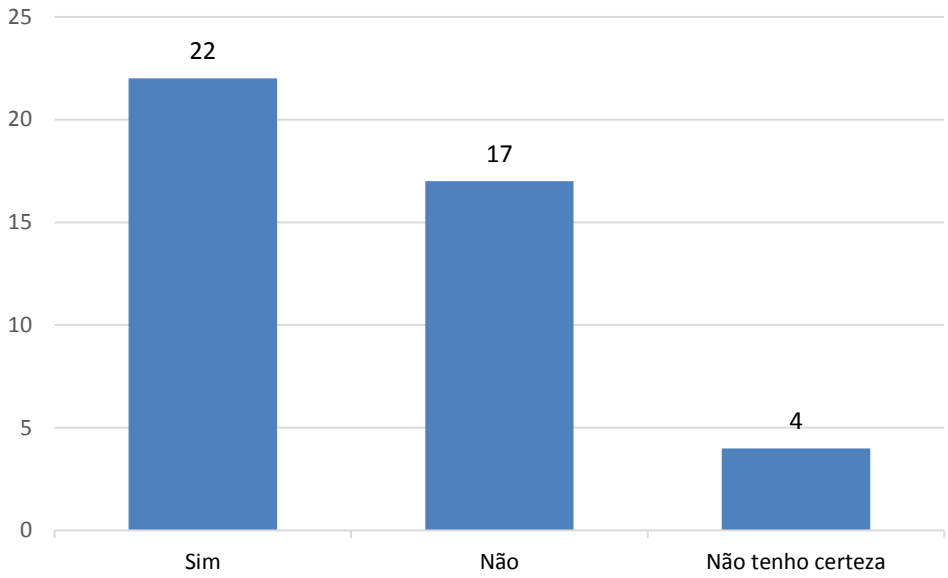
Gráfico 11 – Conhecimento das políticas de segurança utilizadas



Como evidenciado no gráfico 11, a maioria dos colaboradores desconhece as diretrizes adotadas para o acesso e a utilização de informações da companhia, arriscando, ainda que inconscientemente, a segurança dos dados corporativos.

A pergunta seguinte averiguou qual a opinião dos usuários a respeito da intervenção organizacional em seus dispositivos pessoais.

Gráfico 12 - Opinião sobre o controle do BYOD pelas empresas



O gráfico 12 demonstra que os pareceres favoráveis e desfavoráveis estão bastante próximos. Pode-se traçar uma relação entre estes resultados e os obtidos na pergunta anterior, pois se os usuários não conhecem as políticas de segurança da informação da empresa em que atuam, tendem a não compreender a necessidade do controle dos dispositivos.

As perguntas finais da fase direcionada a usuários efetivos verificaram quais pontos os participantes acreditam que sejam influenciados, positiva e negativamente, pelo BYOD. Assim como na indagação sobre as finalidades do uso dos dispositivos móveis, os participantes puderam escolher quantas alternativas desejaram.

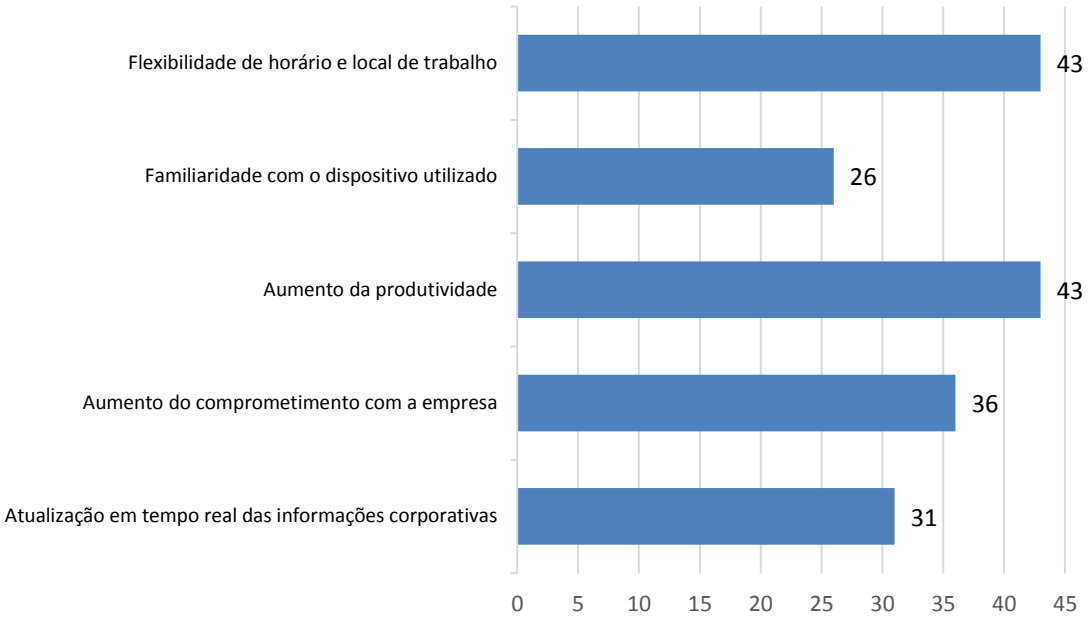
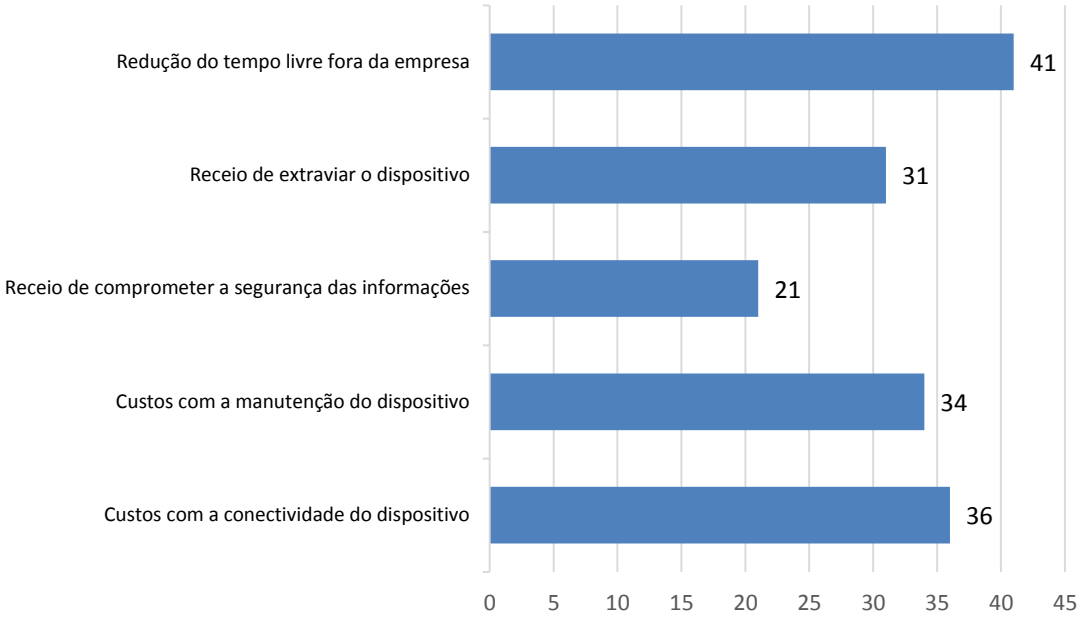


Gráfico 13 – Aspectos positivos do BYOD de acordo com usuários

Por meio do gráfico 13, percebe-se que todos os usuários do BYOD concordam que a prática auxilia no aumento da produtividade e na flexibilidade de horário e local de trabalho. A alternativa menos escolhida foi a familiaridade com o dispositivo utilizado, mas ainda assim foi apontada por mais da metade dos participantes da pesquisa, demonstrando ser um aspecto positivo importante.

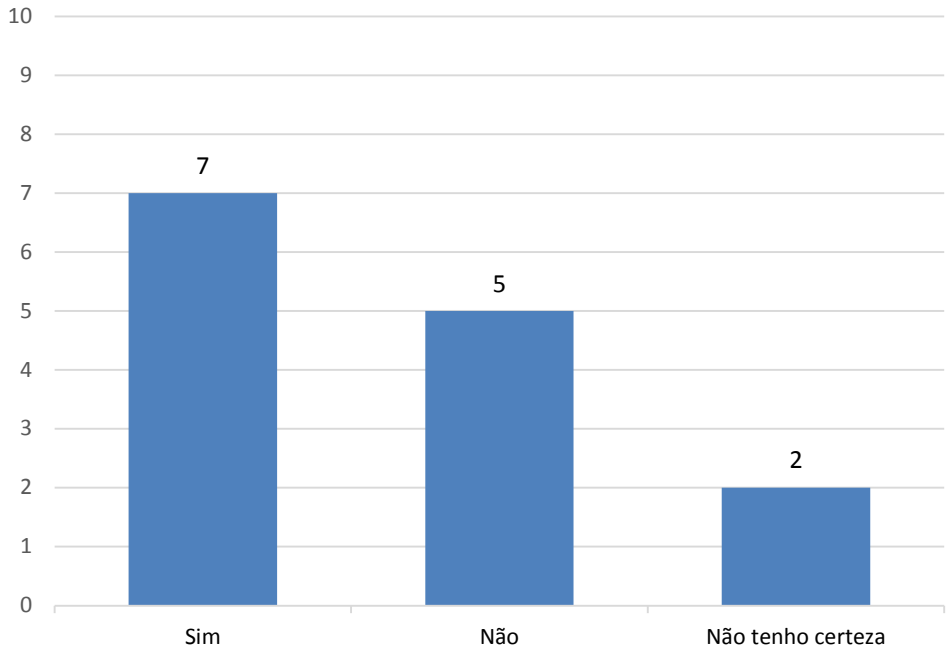
Gráfico 14 – Aspectos negativos do BYOD de acordo com usuários



Novamente evidencia-se, através do gráfico 14, que a segurança da informação não é uma prioridade entre os usuários do BYOD. A principal desvantagem apontada pelos participantes é a redução do tempo livre fora da empresa, seguida das duas alternativas que envolviam custos com conectividade e manutenção.

A última pergunta do questionário, direcionada a indivíduos que ainda não fazem uso de dispositivos móveis pessoais para atividades corporativas é, justamente, se gostariam de aderir à prática. Os participantes que responderam às questões anteriores foram orientados a finalizar a pesquisa.

Gráfico 15 – Interesse em tornar-se usuário efetivo do BYOD



O gráfico 15 demonstra que, dos catorze participantes da pesquisa que não praticam o BYOD, sete gostariam de aderir à tendência. Os cinco indivíduos que alegaram não utilizar dispositivos móveis por opção própria mantiveram sua opinião em não adotar a prática.

Os resultados obtidos com a aplicação do questionário corroboram as referências bibliográficas apresentadas no desenvolvimento deste estudo. A pesquisa demonstrou que o fácil acesso aos dispositivos móveis, efeito do fenômeno da consumerização, têm proporcionado franco crescimento ao BYOD, e que a prática já é comum em muitas empresas.

Entretanto, os usuários ainda desconhecem a importância da segurança da informação, bem como das políticas desenvolvidas para assegura-la, considerando a perda de tempo livre e os custos gerados pelas tendências como as maiores desvantagens ocasionadas pela utilização dos dispositivos móveis.

Por outro lado, o alto índice de participantes que demonstraram ser a favor do BYOD, ainda que não entendam a prática em seu todo, indica que o sucesso da tendência está condicionado à educação dos usuários. Faz-se necessário divulgar e implementar, pelos meios mais didáticos possíveis, boas condutas de segurança da

informação no ambiente corporativo, garantindo que a adesão dos colaboradores derive de um processo não arbitrário, mas consciente.

4 CONSIDERAÇÕES FINAIS

Por meio do fenômeno da consumerização, dispositivos eletrônicos portáteis tais como *notebooks, smartphones* e tablets deixaram de ser itens exclusivos de órgãos governamentais e de grandes corporações, passando a ser ofertados de maneira simples, ágil e em ampla escala ao público em geral. Este acontecimento atenuou a linha divisória entre o público e o privado, tanto em termos de patrimônio físico quanto de capital intelectual, acabando por fundir parcialmente o ambiente organizacional ao particular.

Neste contexto, surgiu o BYOD, *Bring Your Own Device*, que pode ser resumido como a utilização de dispositivos móveis pessoais para a execução de tarefas corporativas. Esta prática tem-se mostrado muito vantajosa para as empresas, que poderão livrar-se de custos com aquisição constante de novos equipamentos, bem como da manutenção dos mesmos, e contarão com funcionários mais eficientes, produtivos e comprometidos. Além disso, os colaboradores também se beneficiam com a utilização de aparelhos com os quais já estão familiarizados e com a flexibilização do horário e local de trabalhos.

Entretanto, o BYOD também possui desvantagens. Os custos que são reduzidos nas empresas podem ser repassados aos empregados, que terão que investir em conectividade e *updates*. A possibilidade de estar sempre *online* também pode reduzir o tempo livre dos colaboradores, refletindo em sua qualidade de vida. O maior ponto negativo, porém, é indubitavelmente a segurança das informações organizacionais. Com mais dispositivos acessando a rede corporativa, aumenta-se o risco de extravio de dados.

Para atenuar possíveis falhas de segurança, é essencial que as corporações planejem a implementação do BYOD, analisando quais as expectativas da empresa com a prática, se o ambiente no qual será adotada é compatível a ela e de quais recursos a organização dispõe. A partir desta análise, deve-se explorar as abordagens viáveis, realizando as adaptações necessárias, e inserir a ferramenta progressivamente, utilizando-se dos *feedbacks* para corrigir erros.

Todas as abordagens consideradas na implementação do BYOD devem considerar o mesmo fator: a gestão da segurança da informação. É necessário

garantir que as informações estejam disponíveis sempre que requisitadas e de maneira autêntica, confidencial e íntegra. Este controle é realizado por meio de políticas de segurança, que podem apresentar-se como manuais de boas condutas e guias de normas técnicas. Considerando que os dispositivos utilizados são pessoais e móveis, as principais políticas de segurança possuem foco em autenticação de usuários e gerenciamento remoto, possibilitando o monitoramento da utilização e a intervenção em caso de falhas.

O BYOD é um fenômeno extremamente dinâmico, pois altera-se no mesmo ritmo irrefreável da evolução tecnológica. Sendo assim, não existe apenas um modo de garantir o sucesso de seu funcionamento, pois cada organização possui um ambiente único, com necessidades e expectativas próprias.

Este estudo pretendeu apresentar alternativas que proporcionem mais benefícios que desvantagens com o uso do BYOD, prezando sempre pela integridade das informações corporativas, um capital inestimável para as organizações. Por meio do questionário realizado, averiguou-se que a prática do uso de dispositivos móveis pessoais para atividades profissionais é muito próxima à relatada em teoria, validando o referencial bibliográfico compilado e, por consequência, atingindo o objetivo do trabalho.

Como sugestão para estudos futuros, recomenda-se a evolução da pesquisa quantitativa para qualitativa, priorizando o levantamento de opiniões mais aprofundadas dos usuários a respeito do BYOD em detrimento de apenas estatísticas. Espera-se que este trabalho, ainda que possa abordar alguns pontos de maneira superficial, seja fonte de apoio aos estudos dos que nele procuram conhecimento.

REFERÊNCIAS BIBLIOGRÁFICAS

ADVISERA. **O que é a ISO 27001?** Introdução simples aos fatos básicos. Disponível em: <https://advisera.com/27001academy/pt-br/o-que-e-a-iso-27001/>. Acesso em: 25 out. 2017.

BANERJEE, Udayan. **What is consumerization of IT?** Disponível em: <https://setandbma.wordpress.com/2012/03/30/consumerization-of-it/>. Acesso em: 09 out. 2017.

BLACKBOX NETWORK SERVICES. **The basics of NAC** – Network Access Control. Disponível em: <https://www.blackbox.nl/_AppData/cms/Default% 20pages/Solutions/Resources/WP%20Veri-NAC_EU.pdf>. Acesso em: 25 out. 2017.

BORRETT, Martin. **Computer fraud&security.** Amsterdã, Holanda, v. 2013, n. 2, p.5-6. 2013. Disponível em: <http://www.sciencedirect.com/journal/computer-fraud-and-security/vol/2013/issue/2>. Acesso em: 07 out. 2017.

BRETERNITZ, V. J.; NAVARRO, F. **Gerenciamento de segurança segundo ITIL:** um estudo de caso em uma organização industrial de grande porte. Revista Eletrônica de Sistemas de Informação. Campo Largo, Paraná, v. 8, n. 2, p.1-15, 2009. Disponível em: <http://www.periodicosibepes.org.br/index.php/reinfo/ article/view/464>. Acesso em: 25 out. 2017.

BRODIN, Martin. **Combining ISMS with strategic management:** the case of BYOD. 8th IADIS International Conference on Information Systems. Funchal, Ilha da Madeira, Portugal, p. 161-168. 2015. Disponível em: <https://www.researchgate.net/ publication/277007918_Combining_ISMS_with_strategic_management_the_case_of _BYOD>. Acesso em: 08 out. 2017.

CASTRO, Yuri M.; SOUZA, Samuel C. **Consumerização de TI:** Solução open-source para gerenciamento de dispositivos móveis em organizações que utilizam BYOD. Disponível em: <https://zenodo.org/record/57614#.WdwlS1tSzIV>. Acesso em: 09 out. 2017.

CERIONI, Thais. **BYOD -** Como preparar seus negócios para uma avalanche de dispositivos. Disponível em: <http://www.la.logicalis.com/globalassets/latin-america/advisors/pt/advisor-byod.pdf>. Acesso em: 09 out. 2017.

CETIC – CENTRO DE ESTUDOS SOBRE AS TECNOLOGIAS DA INFORMAÇÃO E DA COMUNICAÇÃO. **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros** – TIC Domicílios 2015**.** Disponível em: <http://cetic.br/media/docs/publicacoes/2/TIC_Dom_2015_LIVRO_ELETRONICO.pdf >. Acesso em: 05 out. 2017.

CHIARI, Renê. **ITIL Foundation:** o que é ITIL? Disponível em: <https://www.mundoitil.com.br/>. Acesso em: 24 out. 2017.

CISCO SYSTEMS. **Usando VRFs para o isolamento de tráfego.** Disponível em: <https://www.cisco.com/c/pt_br/support/docs/security/nac-appliance-410/112169-nac-layer3-00.html>. Acesso em: 26 out. 2017.

COSTA NOVO, José Procópio da. **Softwares de segurança da informação.** Amazonas: CETAM, 2010. 117p.

CUNHA, I. K. B.; CASTRO, R. C. C. **Gestão da segurança da informação em ambientes BYOD:** um mecanismo de apoio baseado nas boas práticas ITIL. Anais do Encontro Anual de Tecnologia da Informação. Canindé, Brasil, v. 4, n. 1, p.32-39. 2014. Disponível em: <http://www.eati.info/eati/2014/assets/anais/artigo3.pdf>. Acesso em: 24 out. 2017.

DANTAS, Marcus Leal. **Segurança da informação -** uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011. 151p.

DEMING, William Edward. **Qualidade:** a revolução da administração. Rio de Janeiro: Marques-Saraiva, 1990. 367 p.

DIAS, Cláudia. **Segurança e auditoria da tecnologia da informação.** Rio de Janeiro: Axcel Books, 2000. 217p.

DREIBI, Ghassan. **Bring your own device -** que tal levar seus próprios dispositivos para o trabalho? Disponível em: <https://olhardigital.com.br/noticia/bring-your-own-device-que-tal-levar-os-proprios-dispositivos-para-trabalhar/26418>. Acesso em: 10 out. 2017.

ENTERASYS SECURE NETWORKS. **Understanding network access control.** Disponível em: <https://www.techdata.com/techsolutions/networking/files/feb2009/Enterasys%20NAC%20Planning%20Guide.pdf>. Acesso em: 26 out. 2017.

FERREIRA, Fernando Nicolau; ARAÚJO, Márcio Tadeu de. **Política de segurança da informação -** guia prático para elaboração e implementação. 2. ed. Rio de Janeiro: Ciência Moderna, 2008. 224p.

FGV – FUNDAÇÃO GETÚLIO VARGAS. Escola de Administração de Empresas de São Paulo (EAESP). **Pesquisa anual do uso de TI.** Disponível em: <http://eaesp.fgvsp.br/sites/eaesp.fgvsp.br/files/pesti2017gvciappt.pdf>. Acesso em: 05 out. 2017.

FONTES, Edison. **Praticando segurança da informação.** Rio de Janeiro: Brassport, 2008. 308p.

GARANHANI, Bruno. **BYOD -** Bring your own device**.** Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/2520/1/CT_GESER_III_2013_05.pdf>. Acesso em: 09 out. 2017.

GATEWOOD, Brent. **The nuts and bolts of making BYOD work.** The Information Management Journal. Nova York, NY, EUA, v. 46, n. 6, pp. 26-30. 2012.

GOVLOOP. **Exploring bring your own device.** Disponível em: <https://www.govloop.com/blogs/6001-7000/6203-BYODfinal.pdf>. Acesso em: 10 out. 2017.

HARRIS, Jeanne. **IT consumerization –** when gadgets turnin to enterprises IT tools. Disponível em: <https://informationstrategyrsm.files.wordpress.com/2012/09/it-consumerization-when-gadgets-turn-into-enterprise-it-tools.pdf>. Acesso em: 07 out. 2017.

INTEGRITY CONSULTING & ADVISORY. **ISO 27001 -** em que consiste? Disponível em: <https://www.27001.pt/iso27001_3.html>. Acesso em: 25 out. 2017.

INTEL CORPORATIONS. **Insights on the current state of BYOD in the enterprise.** Disponível em: <https://www.intel.com/content/dam/www/ public/us/en/documents/ white-papers/consumerization-enterprise-byod-peer-research-paper.pdf>. Acesso em: 10 out. 2017.

INTERNET BUSINESS SOLUTIONS GROUP – IBSG. **Surveyreport -** BYOD and virtualization**.** Disponível em: <https://www.cisco.com/c/dam/en_us/ about/ac79/docs/BYOD.pdf>. Acesso em: 07 out. 2017.

KOSUTIC, Dejan. **Como obter a certificação ISO 27001?** Disponível em: <https://advisera.com/27001academy/pt-br/blog/2010/12/15/como-obter-a-certificacao-iso-27001/>. Acesso em: 25 out. 2017.

KUMAR, Arun. **Bring your own device (BYOD) advantages and disadvantages.** Disponível em: <http://www.thewindowsclub.com/bring-your-own-device-byod>. Acesso em: 16 out. 2017.

LAUREANO, Marcos AurelioPchek. **Gestão de segurança da informação.** Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_ versao_20.pdf>. Acesso em: 20 out. 2017.

LIEBERMAN SOFTWARE CORPORATION. **BYOD threatanalysis.** Disponível em: <https://liebsoft.com/blog/byod-threat-analysis/>. Acesso em: 16 out. 2017.

MADDEN, Jack. **Think MDM willenable BYOD? Thingagain!** Disponível em: <http://www.brianmadden.com/opinion/Think-MDM-will-enable-BYOD-Think-again-Lets-look-at-the-difference>. Acesso em: 26 out. 2017.

MANSUR, Ricardo. **Governança de TI –** metodologias, frameworks e melhores práticas**.** São Paulo: Brasport, 2007. 200p.

MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito. **Gerenciamento de serviços de TI na prática -** uma abordagem com base na ITIL. São Paulo: Novatec, 2007. 667p.

MATTEUCCI, Gina. **The pros and cons of bring-your-own-device (BYOD for your mobile workforce.** Disponível em: <http://www.msidata.com/pros-and-cons-of-byod-in-mobile-field-workforce>. Acesso em: 16 out. 2017.

MDM SOLUTIONS. **O que é MDM -** a solução. Disponível em: <http://www.mdmsolutions.com.br/o-que-e-mdm/>. Acesso em: 26 out. 2017.

MORETTI, João. **BYOD -** como as empresas devem se precaver. Disponível em: <http://www.tiespecialistas.com.br/2013/02/byod-como-as-empresas-devem-avaliar-e-se-precaver/>. Acesso em 10 out. 2017.

NEAL, Douglas; TAYLOR, John. **The 'consumerization' of information technology.** Disponível em: <https://leadingedgeforum.com/ publication/the-consumerization-of-information-technology-1482/>. Acesso em: 05 out. 2017.

SÊMOLA, Marcos. **Gestão da segurança da informação -** uma visão executiva. 2. ed. São Paulo: Elsevier, 2014. 172p.

STAGLIANO, Thomas; DIPOALO, Anthony; COONELLY, Patricia. **Consumerization of IT.** Disponível em: <http://digitalcommons.lasalle.edu/cgi/ viewcontent.cgi?article=1009&context=mathcompcapstones>. Acesso em: 09 out. 2017.

STONEBURNER, Gary. **Underlying technical models for information technology security.** Washington: U.S. GovernmentPrinting Office, 2015. 24p.

TECHTARGET. **Mobile device management (MDM).** Disponível em: <http://searchmobilecomputing.techtarget.com/definition/mobile-device-management>. Acesso em: 26 out. 2017.

WADLOW, Thomas. **Segurança das redes.** Rio de Janeiro: Campus, 2000. 270p.

WAINWRIGHT, Ashley. **7 benefits of BYOD on enterprise wireless networks.** Disponível em: <https://www.securedgenetworks.com/blog/7-Benefits-of-BYOD-on-Enterprise-Wireless-Networks>. Acesso em: 10 out. 2017.

XCUBE LABS. **MDM -** enable, manage and secure your mobile environment. Disponível em: <https://www.xcubelabs.com/our-blog/enterprise-mobility/mobile-device-management-enable-manage-and-secure-your-mobile-environment/>. Acesso em: 26 out. 2017.

APÊNDICE

QUESTIONÁRIO

Questionário sobre o uso de dispositivos móveis pessoais no ambiente corporativo aplicado por meio de formulário virtual à quarenta e três indivíduos entre os dias 28 e 29 de outubro de 2017. O formulário encontra-se disponível no link <https://goo.gl/forms/dFrbYE3wOCMrvylr2> e, por conta da finalização do estudo, não aceita novas respostas.

Sessão 1 – BYOD (Bring Your Own Device)

Questionário elaborado como parte do Trabalho de Conclusão de Curso para a graduação em Tecnologia da Segurança da Informação da FATEC de Americana/SP. Por gentileza, atente-se às instruções presentes em cada sessão do formulário.

1) Qual é a sua faixa etária?

- ☐ Abaixo de 19 anos
- ☐ 20 – 29 anos
- ☐ 30 – 39 anos
- ☐ 40 – 49 anos
- ☐ Acima de 50 anos

2) Você sabia que o termo empregado para designar a utilização de dispositivos móveis (notebooks, tablets e smartphones) pessoais para atividades profissionais é BYOD (Bring Your Own Device – Traga Seu Próprio Dispositivo)?

- ☐ Sim
- ☐ Não

3) A empresa na qual você trabalha permite o uso de dispositivos móveis pessoais para executar atividades profissionais?

- ☐ Sim
- ☐ Não
- ☐ Não tenho certeza

4) Você utiliza dispositivos móveis pessoais para executar atividades profissionais?

- ☐ Sim
- ☐ Não, pois a empresa na qual trabalho não permite
- ☐ Não, por opção própria

Sessão 2 – Usuários de BYOD

Caso não seja usuário da tecnologia BYOD, apenas clique em "Próxima" no final da página.

5) Qual tipo de dispositivo móvel pessoal você utiliza com mais frequência para atividades corporativas?

- ☐ Notebook
- ☐ Smartphone
- ☐ Tablet

6) Com que frequência você utiliza os dispositivos móveis pessoais para atividades corporativas?

- ☐ Apenas aos finais de semana
- ☐ Apenas em dias de expediente
- ☐ Apenas em emergências e/ou quando solicitado
- ☐ Todos os dias

7) Para quais fins corporativos você utiliza seu dispositivo móvel pessoal? (marque quantas alternativas desejar)

- ☐ Para acessar e redigir e-mails (Outlook, Thunderbird, etc.)

- ☐ Para acessar e redigir apresentações (PowerPoint, Keynote, etc.)
- ☐ Para acessar e redigir planilhas (Excel, Numbers, etc.)
- ☐ Para acessar e redigir relatórios (Word, Pages, etc.)
- ☐ Para acessar softwares próprios da empresa (ERPs)
- ☐ Outros (lista de contatos, folhas de pagamento, etc.)

8) Você possui usuário e senha próprios (não genéricos) para acessar as informações corporativas?

- ☐ Sim
- ☐ Não

9) Você conhece as políticas de segurança da informação utilizadas pela empresa na qual trabalha?

- ☐ Sim
- ☐ Não
- ☐ Não tenho certeza

10) Você acredita que os profissionais de TI e gestores responsáveis devam controlar a utilização dos dispositivos móveis pessoais?

- ☐ Sim
- ☐ Não
- ☐ Não tenho certeza

11) Quais pontos você acredita que são influenciados positivamente pelo uso do BYOD? (marque quantas alternativas desejar)

- ☐ Atualização em tempo real das informações corporativas
- ☐ Aumento do comprometimento com a empresa
- ☐ Aumento na produtividade
- ☐ Familiaridade com o dispositivo utilizado
- ☐ Flexibilidade de horário e local de trabalho

12) Qual pontos você acredita que são influenciados negativamente pelo uso do BYOD? (marque quantas alternativas desejar)

- ☐ Custos com a conectividade do dispositivo (Wi-Fi, 3G, 4G, etc.)
- ☐ Custos com a manutenção do dispositivo
- ☐ Receio de comprometer a segurança das informações da empresa
- ☐ Receio de extraviar o dispositivo (perda, furto, roubo ou dano)
- ☐ Redução do tempo livre fora da empresa

Sessão 3 – Não usuários de BYOD

Caso já tenha respondido às questões anteriores, apenas clique em "Enviar" no final da página.

13) Caso ainda não utilize dispositivos móveis pessoais para executar atividades profissionais, gostaria de utilizar futuramente?

- ☐ Sim
- ☐ Não
- ☐ Não tenho certeza