INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ
TECNOLOGIA EM REDES DE COMPUTADORES

SEBASTIÃO MANFREDO DA COSTA NETO

***BRING YOUR OWN DEVICE* (BYOD)**: POLÍTICAS DE SEGURANÇA NA IMPLANTAÇÃO EM AMBIENTES CORPORATIVOS

MACAPÁ
2021

SEBASTIÃO MANFREDO DA COSTA NETO

BRING YOUR OWN DEVICE (BYOD): POLÍTICAS DE SEGURANÇA NA IMPLANTAÇÃO EM AMBIENTES CORPORATIVOS

Trabalho de Conclusão de Curso apresentado ao curso superior Tecnologia em Redes de Computadores, do Instituto Federal de Educação, Ciência eTecnologia do Amapá como requisitoavaliativo para a obtenção do título de Tecnólogo em Redes de Computadores.
Orientador: Prof. Esp. Francisco Sanches da Silva Júnior.

MACAPÁ
2021

Biblioteca Institucional - IFAP
Dados Internacionais de Catalogação na Publicação (CIP)

C837b Costa Neto, Sebastião Manfredo da
Bring Your Own Device (BYOD): políticas de segurança na implantação em ambientes corporativos / Sebastião Manfredo da Costa Neto - Macapá, 2021.
43 f.: il.

Trabalho de Conclusão de Curso (Graduação) -- Instituto Federal de Educação, Ciência e Tecnologia do Amapá, Campus Macapá, Curso de Tecnologia em Redes de Computadores, 2021.

Orientador: Francisco Sanches da Silva Júnior.

1. Segurança da informação . 2. Tecnologia da informação. 3. Dispositivos móveis. I. Silva Júnior, Francisco Sanches da , orient. II. Título.

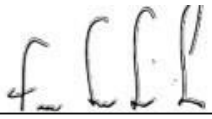
Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica do IFAP
com os dados fornecidos pelo(a) autor(a).

SEBASTIÃO MANFREDO DA COSTA NETO

BRING YOUR OWN DEVICE (BYOD): POLÍTICAS DE SEGURANÇA NA IMPLANTAÇÃO EM AMBIENTES CORPORATIVOS

Trabalho de Conclusão de Curso apresentado ao curso superior Tecnologia em Redes de Computadores, do Instituto Federal de Educação, Ciência eTecnologia do Amapá como requisitoavaliativo para a obtenção do título de Tecnólogo em Redes de Computadores.
Orientador: Prof. Esp. Francisco Sanches da Silva Júnior.

BANCA EXAMINADORA

Francisco Sanches da Silva Junior (Orientador):	
Erika da Costa Bezerra (Examinador I):	
Célio do Nascimento Rodrigues (Examinador II)::	
Sebastião Manfreto Costa Neto (Discente):	

Aprovado em: 04 / 08 / 2021.

Nota: 8,3.

Dedico este trabalho à minha família, amigos e colegas em geral, pelos momentos de ausência.

AGRADECIMENTOS

Certamente estes parágrafos não atenderão a todas as pessoas que fizeram parte dessa importante fase de minha vida. Portanto, desde já peço desculpas àquelas que não estão presentes entre essas palavras, mas elas podem estar certas que fazem parte do meu pensamento e de minha gratidão.

Agradeço ao meu orientador Prof. Esp. Francisco Sanches da Silva Júnior, pela sabedoria com que me guiou nesta trajetória. Aos meus colegas de sala e a Coordenação do Curso, pela cooperação.

Gostaria de deixar registrado também, o meu reconhecimento à minha família, em especial, minha esposa, pois acredito que sem o apoio deles seria muito difícil vencer esse desafio.

Uma máquina consegue fazer o trabalho de 50 homens ordinários. Nenhuma máquina consegue fazer o trabalho de um homem extraordinário.

(HUBBARD, Elbert).

RESUMO

Na fase de consumerização de TI, as organizações permitem que seus funcionários tragam seus dispositivos pessoais para o ambiente de trabalho. Isso é obtido por meio da aplicação de uma política intitulada *Bring Your Own Device*(Traga seu Próprio Dispositivo). As políticas BYOD adotadas em várias organizações, são vagas e geralmente imaturas. Normalmente, não possuem suporte para dispositivos móveis como smartphones, tablets e laptops. Tais políticas de segurança devem ser modificadas para se adequar à inclusão de novos dispositivos. O presente estudo se objetiva no relato das principais políticas de segurança e medidas que podem ser tomadas para garantir a segurança da empresa na BYOD. Para atingir os objetivos do estudo.

Palavras-chave: Bring Your Own Device (BYOD). Políticas de segurança. Consumerização de TI. Dispositivos móveis.

ABSTRACT

In the BYOD phase, organizations allow their employees to bring their personal devices into the workplace. This is achieved by applying a policy entitled Bring Your Own Device. BYOD policies adopted by many organizations are vague and often immature. They typically do not support mobile devices such as smartphones, tablets and laptops. Such security policies should be modified to accommodate the addition of new devices. This study is aimed at reporting the main security policies and measures that can be taken to ensure the company's security at BYOD. To achieve the study objectives.

Keywords: Bring Your Own Device (BYOD). Security policies. IT Consumerization. Mobile device.

LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS

LISTA DE ABREVIATURAS

a.C.	Antes de Cristo
Cód. Civ.	Código Civil
TI	Tecnologia da Informação

LISTA DE SIGLAS

BYOD	Bring Your Own Device
BSC	Balanced Scorecard
CH	Capital Humano
DM	Dispositivo Móvel

LISTA DE ACRÔNIMOS

BYOD	Bring Your Own Device
NASA	National Aeronautics and Space Administration
OTAN	Organização do Tratado do Atlântico Norte

SUMÁRIO

1 INTRODUÇÃO

Atualmente, por conta da grande explosão tecnológica que ocorreu durante os últimos anos, a sociedade e os indivíduos estão desenvolvendo, progressivamente, uma nova dinâmica de se lidar com os dispositivos móveis. Anos atrás, os *smartphones* e notebooks eram considerados artigos de luxo. Entretanto, por conta da evolução do mercado e da capacidade de fabricar dispositivos móveis em larga escala, o uso destes produtos se tornou algo cada vez mais corriqueiro e participante da sociedade como um todo, independente da classe social dos indivíduos. Assim, nos últimos anos, o número de dispositivos móveis cresceu vertiginosamente. Este fenômeno proporcionou grande flexibilização no meio empresarial, já que os usuários podem se utilizar dos seus próprios dispositivos para realizar atividades profissionais dentro e fora do local de trabalho.

Segundo o Relatório de Acompanhamento do Setor de Telecomunicações (2021), da Anatel para o mês de maio de 2021, os indicadores mostram que o Brasil terminou o mês com 241,0 milhões de celulares e densidade de 113,04 Celular para cada 100 habitantes. Para o mesmo período, apresentou adições líquidas de 1,7 milhão de celulares. O pré-pago apresentou adições líquidas de 516 mil celulares. No pós-pago as adições líquidas foram de 1,2 milhão de celulares.

Este fenômeno, é conhecido como *Bring your Own Device* (BYOD), que em sua tradução literal significa “traga seu próprio dispositivo”. O BYOD se trata de uma medida adotada por várias empresas globalmente, de maneira resumida, o BYOD nada mais é do que a utilização do *tablet*, notebook ou *mobile* de uso pessoal para finalidades profissionais, dispensando parcialmente o uso de recursos de infraestrutura da organização.

Essa flexibilização, no entanto, analisada pela ótica da segurança da informação, pode resultar em uma ameaça a privacidade do usuário e a segurança dos dados da empresa. O BYOD, embora apresente maior praticidade e flexibilidade, também demanda rotinas e políticas de segurança, já que o administrador da rede deve manter a integridade das conexões existentes entre os diversos aparelhos buscando o mínimo de incidentes de segurança possíveis. Assim, nota-se que o BYOD demanda mudanças e/ou adaptações na política de segurança utilizada na infraestrutura computacional e organizacional das empresas.

A partir do exposto, este estudo busca analisar os diversos cenários e

possibilidade direcionadas à segurança da informação com a utilização do modelo BYOD nas organizações, comparando suas vantagens e desvantagens, bem como as necessidades inerentes a sua implementação.

Para este estudo, a revisão bibliográfica foi o método principal de norteamento das analise e considerações apresentadas ao longo do documento. A revisão bibliográfica localiza o problema de pesquisa dentro da obra de outros autores com a finalidade de se encontrar parâmetros e critérios que fundamentem o trabalho e ergam bases para o estudo.

A pesquisa bibliográfica, considerada uma fonte de coleta de dados secundária, pode ser definida como: contribuições culturais ou científicas realizadas no passado sobre um determinado assunto, tema ou problema que possa ser estudado (LAKATOS e MARCONI, 2001).

Para Lakatos e Marconi (2001, p. 183), a pesquisa bibliográfica,

> [...] abrange toda bibliografia já tornada pública em relação ao tema estudado, desde publicações avulsas, boletins, jornais, revistas, livros, pesquisas, monografias, teses, materiais cartográficos, etc. [...] e sua finalidade é colocar o pesquisador em contato direto com tudo o que foi escrito, dito ou filmado sobre determinado assunto [...].

Em suma, todo trabalho científico, toda pesquisa, deve ter o apoio e o embasamento na pesquisa bibliográfica, para que não se desperdice tempo com um problema que já foi solucionado e possa chegar a conclusões inovadoras (LAKATOS e MARCONI 2001).

Segundo Vergara (2000), a pesquisa bibliográfica é desenvolvida a partir de material já elaborado, constituído, principalmente, de livros e artigos científicos e é importante para o levantamento de informações básicas sobre os aspectos direta e indiretamente ligados à nossa temática. A principal vantagem da pesquisa bibliográfica reside no fato de fornecer ao investigador um instrumental analítico para qualquer outro tipo de pesquisa, mas também pode esgotar-se em si mesma.

No presente trabalho, serão apresentadas informações sobre BYOD e as políticas de segurança que garantam o funcionamento íntegro do referido mecanismo.

2 DISPOSITIVOS MÓVEIS

Os dispositivos móveis (DM) podem ser caraterizados de forma genérica como tecnologias com alta mobilidade que desempenham funções computacional em equipamento embarcados, com a presença de processamento, armazenamento e conectividade semelhantes aos computadores tradicionais. Pelo nível de tecnologias envolvidas e pela variedade dos tipos de "*devices*" (termo na língua inglesa) que podem ser considerados como DM, uma definição para está modalidade de ferramenta é mais complexa do que parece. Contudo, alguns autores evidenciarão a seguir algumas características que facilitarão o entendimento e abrangência desta temática.

Segundo Malathy e Kantha (2013, p. 362), "com diferentes tipos, estilos, modelos, "diferentes capacidades e funções embutidas como câmeras, telas de toque, leitura de código de barras, rede sem fio, bluetooth, mensagens, GPS, RFID, sistemas operacionais".

São muitos os aparelhos que podem ser classificados como DM. Podem ser "smartphones, videogames, câmeras digitais, media players, netbooks, GPS, computadores de mão" afirma Traxler (2010, p. 149- 150).

Segundo Zhong (2013, p. 1742) identifica os DM como "dispositivos de mídia móvel" (MMDs), representados pelos "smartphones, tablets, iPads". Para o autor são tecnologias fomentadoras dos laços sociais que apresentam aos usuários novas formas de interagir com a informação.

Partindo destas contextualizações, podemos vislumbrar em nossa realidade cotidiana, quais equipamentos podemos caracterizar como dispositivos móveis, e quais deles, poderiam ser utilizados como uma ferramenta profissional, sendo utilizada dentro do ambiente de trabalho, aliando, comodidade, praticidade e familiaridade no uso de softwares e mecanismos que auxiliem na produtividade individual em um ambiente coorporativa.

3 *BRING YOUR OWN DEVICE* (BYOD)

Conceitualmente, é possível descrever o *Bryng Your Own Device* (BYOD) como a utilização de dispositivos pessoais para finalidades profissionais. Neste modelo, o funcionário pode ter acesso à dados corporativos de qualquer dispositivo móvel, como notebook, *tablet* ou *smartphone*. Uma pesquisa realizada por Morrow (2012) afirma que os dispositivos eletrônicos estão cada vez mais sendo utilizados para realizar demandas profissionais. A partir disto, o indivíduo tem uma maior flexibilidade em escolher o dispositivo que mais lhe agrada para a realização de tarefas profissionais, optando pelo modelo ou marca que mais se adapta às suas necessidades.

De acordo com Thomson (2012), esse tipo de mudança empresarial é conveniente para a empresa por conta das reduções de custos que isto implica, já que o usuário é integralmente responsável pelo o seu dispositivo. Entretanto, o autor também alerta que um dos principais pressupostos do *BYOD* é que o dispositivo do usuário deve se adaptar às políticas de segurança que são predeterminadas pelo administrador da rede.

Analisando as medidas do BYOD por um viés restritamente econômico, é possível afirmar que esta medida é uma via de mão dupla: ao mesmo tempo em que a corporação possui redução de gastos econômicos relativos ao *hardware*, ela concomitantemente tem que realizar maiores investimentos em *software* e na infraestrutura de TI. Estes investimentos, longe de serem feitos apenas no *software* em si, também têm de ser realizados em uma mão de obra capacitada para operar e planejar o sistema, pois os profissionais devem ser capazes de manter o desempenho do sistema nas mais diversas plataformas utilizadas pelos funcionários.

Além do que foi afirmado, o BYOD também demanda maiores investimentos na segurança de informação. De acordo com Sommerfeld (2015), esta medida inevitavelmente facilita o vazamento de dados da empresa, pois por questões de privacidade dos funcionários, os dispositivos não podem ser diretamente gerenciados pelos administradores da rede, já que eles também são simultaneamente de uso pessoal. De acordo com o autor supracitado, o BYOD também dá a possibilidade de acontecer um evento muito recorrente em empresas que adotam este método, que é o *Shadow IT* (ou TI Invisível

Segundo Sommerfeld (2015), o *shadow IT* nada mais é do que o acesso aos dados da nuvem sem que haja o conhecimento prévio da empresa. Assim, o

funcionário, a partir do seu próprio dispositivo, pode acessar os dados da nuvem para diversos objetivos, desde o gerenciamento de sua própria agenda até o planejamento de tarefas. Todavia, em alguns casos os dados acessados não estão corretamente protegidos. Segundo Perini (2017), isto ocorre principalmente em casos onde a empresa não consegue fornecer ao funcionário todas as soluções e meios necessários para o acesso de arquivos. Assim, o funcionário acaba utilizando aplicativos de terceiros que podem não possuir a segurança necessária.

3.1 Vantagens e desvantagens

Toda proposição de inovação organizacional em uma organização, apresenta desafios e benefícios, uma vez que existe uma equidade a longo prazo dos benefícios em detrimento do uso de uma nova solução, aliada esta, ao crescimento empresarial no setor do qual o seguimento do negócio está inserido.

De acordo com Perini (2017), as vantagens da adoção do *BYOD* são as seguintes:

- Diminuição de custos por parte da empresa, principalmente em microempresas que precisam operar com um orçamento restrito;
- Possibilidade de o funcionário escolher a tecnologia que mais se adequa as suas necessidades e gostos, melhorando o seu bem estar e satisfação durante a jornada de trabalho;
- Possibilidade de inovação por parte dos funcionários, já que ele pode utilizar novas tecnologias ou métodos para alavancar a sua produtividade;
- Promoção da solução autônoma do funcionário, já que ele fica livre para escolher qual método melhor se adequa à resolução do problema que está envolvido no seu trabalho.

Quanto às desvantagens, Perini (2017) elenca os seguintes pontos:

- Por conta da flexibilização dos dispositivos, o setor de TI tem de lidar com maiores desafios relativos à privacidade e segurança dos dados do usuário e da empresa;
- As informações corporativas têm de ser mais restritas e controladas

pelos administradores do sistema;

- O departamento de TI tem de elaborar um relatório com todos os dispositivos que possuem acesso às informações da empresa, mantendo a lista atualizada de acordo com o nível de acesso que os funcionários respectivamente possuem aos dados corporativos;
- Por conta da diversidade de dispositivos que podem ser utilizados, os administradores podem ter problemas com desempenho e compatibilidade entre o sistema de TI e o sistema operacional do dispositivo usado pelo funcionário.

3.2 O BYOD e a utilização do BYOS

Além da flexibilização dos dispositivos proporcionados pela BYOD, algumas empresas adotam políticas ainda mais flexíveis, como o BYOS (*Bring Your Own Software*). A BYOS permite que o funcionário utilize softwares ou tecnologias de sua própria escolha para a resolução das tarefas profissionais. Dentre essas tecnologias, Taurion (2009) elenca, por exemplo: virtualização do desktop, virtualização de aplicações e a computação em nuvem.

Dentre as tecnologias elencadas anteriormente, Taurion (2009) afirma que a computação em nuvem é a mais comum delas. De acordo com o autor, a computação em nuvem nada mais do que um ambiente de computação formado por diversos servidores diferentes, sejam eles físicos ou virtualizados. Assim, a computação em nuvem possui a finalidade de disponibilizar ao funcionário informações e dados corporativos através de dispositivos pessoais, para que eles possam ter acesso a esses dados sem necessariamente estarem presentes no ambiente de trabalho.

A virtualização de aplicações, por sua vez, é a criação de uma espécie de “escritório remoto”. De acordo com a CIO (2016), quando a aplicação não possui uma interação eficaz com o *kernel* do sistema, o usuário pode optar por “virtualizar” a aplicação, gerando um maior flexibilização e praticidade. Para a virtualização de aplicações, o *software* se utiliza do processamento de um dispositivo de destino, como um PC ou *notebook*.

Por fim, a virtualização do desktop (também conhecido como máquinas virtuais) é a tecnologia responsável por emular uma máquina na rede se utilizando de servidores disponibilizados pela própria corporação. Através da virtualização do desktop, o usuário pode acessar os dados diretamente do servidor sem ter de utilizar

uma máquina que esteja fisicamente conectada à ele. Segundo Perini (2017), essa tecnologia, assim como as demais, também permite um melhor gerenciamento e acesso aos administradores.

De acordo com Delaney (2012), a criação de máquinas virtuais geralmente é realizada com base em modelos de sistemas operacionais pré-definidos, que comumente já possuem *softwares* e configurações de rede pré-programadas. O autor supracitado afirma que as corporações geralmente possuem seus próprios protocolos de comunicação para que o funcionário possa acessar os dados através de uma maquina virtual. Dentre os protocolos, os mais utilizados são o *Virtual Private Network* (VPN) e o *Mobile Device Management* (MDM).

De acordo com Delaney (2012), a VPN cria a possibilidade de comunicação entre várias máquinas de maneira simultânea através da Internet, criando uma teia que interconecta as respectivas máquinas ao mesmo tempo em que criptografa os dados e a sua integridade. A MDM, por sua vez, é mais utilizada para dispositivos móveis, sendo um conglomerado de tecnologias que possuem a finalidade de gerenciar os dispositivos e a sua respectiva conexão com um determinado servidor, que geralmente é a nuvem (DELANEY, 2012).

Earls (2015) afirma que quando a empresa opta pela adoção do BYOS, é interessante que ela desenvolva padrões de segurança voltados para o *Data Loss Prevention* (prevenção de perda de dados). A partir da estratégia elencada, a empresa pode diminuir exponencialmente a possibilidade de ataques ao servidor e de vazamento de informações sigilosas. Earls (2015) afirma que o *Data Loss Prevention* é uma tática utilizada para detectar tráfego de dispositivos estranhos à rede, bloqueando o acesso aos dados. A partir disso, a empresa pode evitar que *smartphones* conectados ao sistema possa vazar dados da corporação.

3.3 Segurança da informação

Dentro do contexto do BYOD, se faz com muito rigor, analisar os conceitos de segurança que serão cruciais para a aplicação deste modelo de utilização, sem comprometer a infraestrutura organizacional, trazendo riscos para a gestão dos ativos empresariais.

> A segurança da informação busca proteger a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, visando minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio. O sistema de proteção da informação deve considerar aspectos ligados a: segurança física da informação, segurança lógica, segurança das relações financeiras, garantia da reputação e imagem da organização, aspectos legais, comportamento dos funcionários, e para com os funcionários, e todos os ativos tangíveis e intangíveis (PELTIER,2001).

Segundo Torres, Carvalho, Silva (2003, p. 17), A preservação da confidencialidade, integridade e disponibilidade da informação utilizada nos sistemas de informação requer medidas de segurança, que por vezes são também utilizadas como forma de garantir a autenticidade e o não repúdio.

> A implementação do sistema de proteção da informação deve transpor as fronteiras da implantação de dispositivos de hardware ou software, que protegem o que está armazenado nos bancos de dados e arquivos da empresa, e muitas vezes não oferecem a segurança necessária ou esperada devido a falhas de funcionamento ou de parametrização e instalação (PELTIER, 2001).

Segundo Torres, Carvalho, Silva (2003, p. 17), Um Programa de Segurança bem estruturado deverá reduzir as vulnerabilidades dos sistemas de informação e fazer evoluir as suas capacidades de inspeção, detecção, reação e reflexo, assentando num conjunto universal de princípios que garanta o seu equilíbrio e eficiência.

3.3.1 Segurança em BYOB

De acordo com Santos (2017), a criação de regras de conduta e políticas de segurança são de elementar importância para que a corporação possa ter um certo controle sobre os dados que os funcionários possuem acesso. Além disso, é necessário um processo de conscientização que ensine os funcionários que as informações da empresa são um dos principais ativos de valor. Assim, as informações devem ser guardadas de maneira rigorosa, sendo o funcionário um dos principais responsáveis de preservar a integridade das informações que ele possui acesso.

Cometti (2016) explica que as políticas de segurança possuem a finalidade de regrar as atividades dos seus respectivos colaboradores. Destarte, essas normas devem ser de conhecimento unívoco de todos os indivíduos que atuam na corporação.

Para aumentar a penetrabilidade e o conhecimento destas normas pelos funcionários, Cometti (2016) afirma que as regras devem ser as mais claras e compreensíveis possíveis.

Além das medidas supracitadas, Cometti (2016) também ressalta a importância da realização do monitoramento da entrada e saída de dados em todos os setores possíveis independente da hierarquia dos funcionários. O monitoramento é de grande utilidade caso a empresa caia no infortúnio de um vazamento de dados. Através do monitoramento, é possível rastrear a origem de saída dos dados e o dispositivo utilizado. Esta ação é necessária por que atualmente, toda empresa que trabalha com uma grande quantidade de dados está suscetível à fraudes e furtos de dados.Segundo Santos (2017), o vazamento de dados pode causar grande prejuízos às empresas. Quanto às causas, Santos (2017) elenca a origem do vazamento de dados como ausência de controle quanto ao fornecimento de dados.

Sendo assim, a segurança no BYOD tem um grande envolvimento com o risco das intenções humanas. Funcionários mal intencionados podem facilmente vazar projetos, segredos de mercado que possuem propriedade intelectual, ou outros tipos de informações sensíveis, salvando os dados em qualquer fonte de armazenamento, desde a nuvem até dispositivos físicos. Além dos funcionários mal intencionados, a empresa também pode lidar com usuários que não tem conhecimentos de segurança dos dispositivos móveis, que pode realizar o vazamento de maneira não intencional. Assim, além da precaução que a empresa deve ter quanto à idoneidade dos seus funcionários, ela também deve realizar programas de capacitação para prevenir vazamentos acidentais ou intencionais (MORROW, 2012).

Uma recente pesquisa realizada pelo Programa de Analista SAANS (2013) em muitas organizações empresariais sobre a criticidade da Política de Segurança Móvel, identificou que 97% da organização acredita que as políticas de segurança BYOD são importantes.

Mas a questão é se eles realmente seguem a política BYOD. De acordo com pesquisa do Programa de Analista SAANS, 36% da organização não tem uma política formal de BYOD; 23% das empresas não permitem dispositivos pessoais e 14% da organização informa seus funcionários para proteger e monitorar seus próprios dispositivos (JOHNSON E LAGRANGE, 2013).

Os dispositivos de root ou *jailbreak* são capazes de usar o sistema operacional com permissão de administrador. Estes tipos de dispositivos não são tão largos e são

menos de 2% disponíveis na indústria, mas isso deve ser considerado seriamente (VIGNESH E ASHA, 2015).

Os dispositivos com root são capazes de instalar aplicativos não autorizados que podem exibir spam e enviar dados anônimos sobre o dispositivo. O número do celular usado no dispositivo deve ser verificado, a fim de confirmar que o funcionário é o dono do número. Os aparelhos smartphone podem ser protegidos por senha. Isso fará com que esteja protegido fisicamente. Slots de memória estão disponíveis nesses telefones contendo cartões de memória. Esses cartões podem ser roubados, o que resulta facilmente na violação de dados. Existem alguns problemas de compatibilidade quando os dispositivos trabalhando em diferentes sistemas operacionais. Este problema deve ser resolvido para tornar flexível a escolha dos dispositivos (VIGNESH E ASHA, 2015).

Existem algumas soluções para os problemas de segurança. Senhas fortes são recomendadas para bloquear os dispositivos que fornecem à segurança. Os desktops virtuais são substituídos para impedir que se salvem os dados no dispositivo. Isso fará com que o funcionário trabalhe apenas online. O trabalho offline não é possível quando desktops virtuais são usados. Gerenciamento de dispositivos móveis que ajudam o proprietário do dispositivo a alterar as senhas periodicamente e limpar remotamente quando as senhas são digitadas incorretamente. A produtividade do funcionário não diminui com o aumento da segurança através de restrições (VIGNESH E ASHA, 2015).

3.3.2 Ataques de vírus

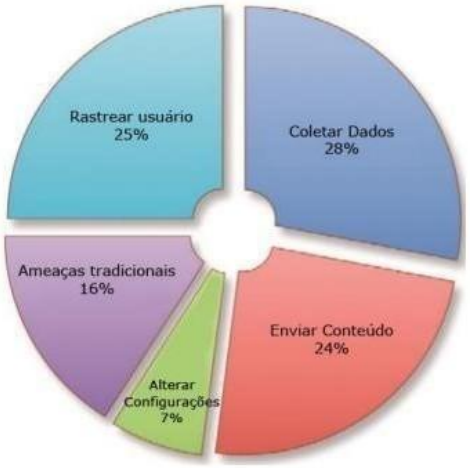
Entretanto, é necessário se ter em mente que o vazamento de dados nem sempre ocorre de maneira maliciosa, isto é, realizado com intenções secundárias por parte dos funcionários da empresa. Segundo o relatório do *International Journal in IT and Engineering*, atualmente, o BYOD apresenta quatro grandes vulnerabilidades, que são, a saber: *malwares*; ausência de controle quanto à permissão de acesso do usuário; falhas na encriptação e mal uso dos dados por parte do usuário. Outra pesquisada realizada por Morrow (2012) aponta que pelo menos 47% dos funcionários que se utilizam do BYOD, acessam as informações corporativas através do seu desktop pessoal; 41% realiza o acesso através dos *notebooks*; 24% através dos seus *smartphones* e 10% através dos tablets.

Entretanto, em alguns dos casos, os dispositivos pessoais não possuem nem sequer sistemas básicos de segurança que garantam a integridade do acesso. Por conta da ausência de segurança, a maioria dos dispositivos estão suscetíveis à ataques cibernéticos. Esta falta de dispositivos de segurança tornam os dispositivos passíveis de ataques de *malwares*, *keyloggers* e outros tipos.

De acordo com Isaca (2016), os *malwares* nada mais são do que softwares de cunho malicioso que são desenvolvidos por hackers para diversos fins. Dentre os diversos tipos de *malwares* existentes, Isaca (2016) cita os *spywares*, *adwares* e o cavalos de tróia. Os *spywares* são vírus responsáveis por colher informações do usuário do dispositivo, como conteúdos acessados na internet e outras preferências pessoais; os *adwares* são vírus responsáveis pela reprodução de propagandas no dispositivo; os cavalos de tróia, por fim, são programas responsáveis por criar portas de entrada que facilitam a invasão dos vírus no dispositivo.

A figura elaborada pela Symantec (2011) ilustra os principais danos que estes vírus causam em *smartphones* (figura 1):

Figura 1 - Efeitos do *malware* nos *smartphones*



Fonte: (SYMANTEC, 2011)

Segundo uma pesquisa realizada pela *Computer World* em 2016, os *smartphones* estão sendo cada vez mais utilizados no cotidiano, atingindo a quantidade de 3.8 milhões no ano da referida pesquisa (COMPUTER WORLD, 2016). Destarte, por conta da grande usabilidade dos *smartphones*, existem cada vez mais indivíduos utilizando-os para fins profissionais.

Por conta do grande crescimento, também há um maior interesse por parte dos

hackers em criar vírus que possuam maior penetrabilidade nestes dispositivos, os utilizando para o roubo e coleta de dados pessoais e corporativos. De acordo com Morrow (2012), a maior parte dos vírus são criados tendo como o alvo a plataforma *Android*, já que ela é atualmente uma das mais utilizadas. O autor supracitado elenca que o descuido do funcionário pode prejudicar a empresa. Um exemplo dado pelo autor é que o funcionário pode vazar informações sigilosas apenas por ter acessado a rede corporativa e armazenado alguma informação em seu dispositivo local. Caso o dispositivo esteja infectado por algum destes vírus, a informação inevitavelmente irá ser transmitida à terceiros. Além do armazenamento local, o *malware* também tem a possibilidade de invadir outros dispositivos de armazenamento, como cartões micro SD e HD's externos.

Perini (2017) elenca que existem outras possibilidades de vazamento de informações além da internet. De acordo com o autor, o *bluetooth* também é um dos meios de transmissão que podem ser utilizados para o roubo de informações. De maneira resumida, o *bluetooth* possui a finalidade de realizar um pareamento entre dispositivos móveis. O pareamento é realizado através da emissão de uma frequência que é criptografada, possuindo uma chave de acesso que permite que um dispositivo possa se conectar a outro. O conhecimento da chave, para Perini (2017), é um dos principais meios utilizados por hackers para ter acesso às informações transmitidas entre os celulares.

Além das possibilidades de transmissão citadas anteriormente, existem diversas outras fraquezas dos dispositivos móveis que podem ser exploradas, como os ataques de negação de serviço (PERINI, 2017).

3.3.3 Medidas de segurança em dispositivos móveis

As medidas elencadas no presente tópico, de maneira geral, são majoritariamente de responsabilidade do usuário, servindo tanto para indivíduos que utilizam seu *smartphone* ou dispositivo móvel para uso pessoal quanto para uso profissional. Conforme explicado no tópico anterior, o crescimento exponencial dos dispositivos móveis fomentou ainda mais a indústria dos hackers. De acordo com uma pesquisa realizada pela Synnex Westcon (2016), a grande maioria do vazamento de informações acontece por conta de vírus e outras espécies de *malwares*. Quanto às causas da invasão dos vírus, é possível citar a ausência de programas de segurança

ou de atualizações no sistema operacional. Segundo a Synnex Westcon (2016), os meios que os vírus se utilizam para invadir os dispositivos móveis geralmente são pela instalação de *softwares* ou aplicativos de lojas não oficiais, SMS ou *pishing*, que se trata de um método de fraude online que possui a finalidade de roubar informações pessoais, como senhas de email, bancos, dentre outras informações.

Assim, de maneira geral, existem medidas que podem ser tomadas pelo usuário que não necessariamente envolvem soluções técnicas ou instalação de aplicativos de segurança. Embora as medidas supra elencadas sejam recomendáveis, existem medidas mais básicas que estão ao alcance de qualquer usuário. Dentre estas medidas, o funcionário pode, por exemplo, evitar instalar aplicativos de origem não conhecidas em seu celular (SYNNEX WESTCON, 2016).

Além do roubo de informações causado por vírus, existem outros métodos que não necessariamente se utiliza deste meio, que é o *pishing*. O *pishing*, de maneira resumida, é quando um indivíduo se passa por uma empresa ou pessoa confiável e pede dados sigilosos ao usuário. Assim, além de não instalar aplicativos, o usuário também deve tomar cautela com a comunicação com usuários que se passem por empresas ou pessoas. Segundo Santos (2017), as empresas geralmente não costumam mandar mensagens pedindo senhas ou qualquer categoria de dados sigilosos do usuário.

O SMS, junto com os métodos elencados anteriormente, também é um dos meios utilizados por hackers para a invasão de dispositivos móveis. Através do SMS, o hacker pode, por exemplo, enviar links de cunho duvidoso que, ao serem acessados, infectam o dispositivo com vírus (SANTOS, 2017).

O usuário do dispositivo móvel também deve tomar cuidado com locais que possuem redes de Wi-fi públicas, como lanchonetes, restaurantes, praças, shoppings e aeroportos, De acordo com a Synnex Westcon (2016), existe o risco de indivíduos mal intencionados se utilizaram destas redes públicas como locais para implantar pontos de acesso wi-fi falsos.

Assim, a partir do que foi elencado até o presente momento, o usuário, junto com a empresa, é um dos grandes responsáveis por resguardar a integridade das informações que ele possui acesso. Todas as informações que foram citadas devem fazer parte do treinamento dos funcionários, já que a desinformação também é um dos grandes canais que os hackers e outras pessoas mal intencionadas se utilizam para praticar os seus ataques.

Além do que foi citado, Santos (2017) também cita uma série de medidas que devem ser tomadas pelo usuário, que são, a saber:

- Instalar programas de antivirus no dispositivo que permaneçam operantes durante a maior parte do tempo de uso do mesmo. Os programas de antivírus, atualmente, contam com uma série de utilidades que são benéficas ao usuário, como otimização do desempenho, mecanismos de bloqueio de *pop-ups*, bloqueio contra spam e programa antirroubo que salvaguarda as informações do usuário;
- Realizar, periodicamente, alteração das senhas de email e outras aplicações que necessitam de senha. Westcon (2016) afirma que é conveniente que o funcionário altere as suas senhas de três em três meses, s utilizando de símbolos, números e combinações de letras;
- Além de tomar cuidado com links enviados por SMS, o usuário também deve ter cuidado ao abrir e-mails que lhes são enviados. Os e-mails, assim como outros canais de informações utilizados nos *smartphones*, não estão imunes à ataques. Através dos e-mails, é possível anexar links que possuam *trojans* e outros tipos de vírus. Destarte, o usuário deve ter cuidado ao checar e-mails de remetentes ou contatos desconhecidos;
- Tomar cuidado ao realizar compras em sites que pedem dados sigilosos como senhas de cartão de crédito. O funcionário deve optar por meios de pagamento seguro, um exemplo dado por Westcon (2016) é o *Google Pay*;
- Tomar cautela na navegação feita na internet. Existem sites que possuem vírus específicos para infectar dispositivos móveis.

3.4 O BYOD à nível organizacional

As medidas que foram elencadas anteriormente, embora sejam eficazes, são sumariamente destinadas aos funcionários e as classes mais basilares da empresa. Todavia, existem algumas medidas que também devem ser tomadas pela empresa para a manutenção da segurança do sistema.

De acordo com Junior (2013), coadunando com tudo o que foi exposto até opresente momento, as regras de adoção da BYOD não podem ser demasiadamente complexas. Destarte, a empresa deve definir de maneira clara o que poderá ser acessado, quem poderá acessar, quando poderá ser acessado e como o acesso será

feito. Assim, a empresa deve cuidar de uma série de fatores condicionantes para que o acesso possa ocorrer. Entretanto, para que isto seja possível, Junior (2013) afirma que a empresa deve realizar um mapeamento para definir as melhores soluções para a sua rede

Perini (2017) afirma que outro fator de extrema importância é a compreensão da empresa sobre quem são os seus usuários e quais dispositivos são os mais utilizados na empresa, ajudando na classificação de equipamentos e políticas. Logo então, mapear os tipos de usuários, tipos de acesso e necessidades de cada um é necessário para que a empresa possa compreender a lógica de operação de seus usuários. Em acréscimo ao que foi afirmado por Perini (2017), Junior (2013) afirma que a empresa deve ter um relatório dos usuários que possuem acesso à informações críticas da empresa, conhecendo também o dispositivo utilizado pelo usuário. De acordo com o autor supracitado, o conhecimento do dispositivo assegura que a empresa possa ter um maior controle quanto ao ataque de vírus e outras fragilidades do sistema.

De acordo com a Teltec Solutions (2013), outra medida elementar para a segurança no BYOD à nível organizacional é a classificação das informações que a empresa possui. Assim, para que a empresa possa assegurar a segurança dos dados, é necessário que ela classifique as suas informações em diferentes níveis de sigilo, pois dependendo da criticidade da informação, a empresa pode optar que elas possam ser acessadas apenas por dispositivos disponibilizados pela própria empresa.

O órgão supracitado também elenca a necessidade de dividir as informações pessoais e as informações corporativas. Para um melhor manejo dessas informações, é recomendado que a empresa opere apenas com um servidor, optando por um serviço de soluções em nuvem que possua um gerenciamento de informações prático.

Conforme se elencou ao longo dos tópicos anteriores, o treinamento é uma fase essencial em qualquer empresa. Destarte, a empresa deve possuir investimentos significativos para fazer com que os usuários conheçam as políticas internas da empresa quanto ao BYOD, expondo suas respectivas proibições e os resultados inerentes aos excessos cometidos pelo setor. De acordo com Junior (2013), é interessante que o gestor da organização aproxime o setor de TI ao setor de recursos humanos, criando uma estratégia para dispositivos perdidos, roubados e para funcionários que saem da empresa.

Além de tudo o que foi elencado, um dos melhores investimentos que a

empresa pode fazer é investir no próprio estudo do assunto, observando como outras empresas conseguem usufruir dos benefícios proporcionados pelo BYOD (JÚNIOR, 2013).

3.4.1 Configurações da rede para BYOD

Júnior (2013, p. 27) elenca algumas opções de configurações de rede e outras medidas que podem ajudar na usabilidade do BYOD à nível organizacional:

- VPN: é uma rede privada, que pode conter protocolos de criptografia, com a finalidade de estabelecer uma ligação virtual entre dois pontos para troca de informações de modo seguro. O uso de VPN garante mais segurança na troca de informação dos dispositivos com a empresa.
- VLAN: O uso de VLAN permite criar redes logicamente independentes. Um ponto importante para o uso de VLAN é que se pode restringir acesso a recursos de rede, com isto pode-se também separar a rede corporativa da rede de acesso comum. Deve ser configurada nos dispositivos da empresa.
- Controle de dispositivos por MAC: O Media Access Controle (MAC) é o endereço físico que cada interface de comunicação em um dispositivo contém. Não é o modo mais seguro, e deve ser utilizado sempre associado a algum outro método, mas de forma simples e acessível, permite o mapeamento de dispositivos e autorização de somente dispositivos conhecidos acessarem a rede corporativa;
- Autenticação: utilizar sistemas que permitam identificar todos os acessos, quem acessa e o tipo de informação, às redes corporativas. A autenticação deve existir para acesso a aplicações, acesso a servidor. Outro ponto importante é autenticação da rede wireless, de preferência por usuário, através de servidor Radius, também conhecido como IEEE 802.1x, por exemplo.
- IEEE 802.1x: é um link padrão de autenticação de camada de controle de acesso baseadas em portas. O IEEE 802.1X é utilizado para adicionar autenticação baseados no usuário com RADIUS e EAP suporte para redes wireless para maior segurança. O padrão identifica e autentica os usuários antes de conceder acesso à rede.
- ACL: access control list (ACL) é um termo utilizado para definir permissão de acesso a certos serviços, aplicações ou conexão de rede. O uso de ACL pode ser utilizado em acesso a aplicações, para que o acesso às informações só seja

permitido àqueles usuários que realmente estão habilitados; Em redes, o uso de ACL pode ser utilizado em switches ou roteadores, com o intuito de regras de classificação de tráfego, seja por porta, por endeço de IP (Internet Protocol) ou por protocolo.

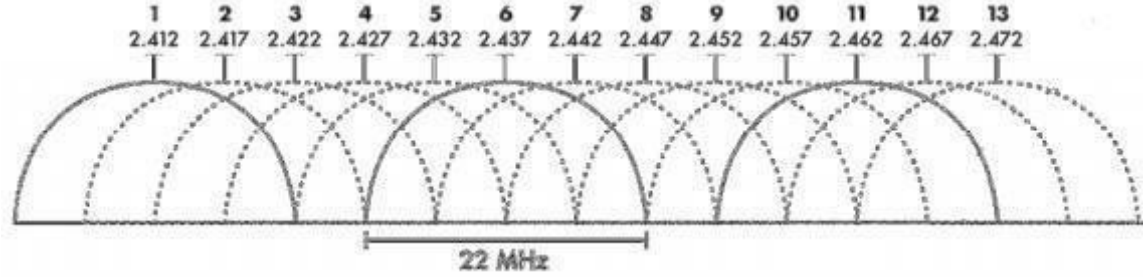
- Monitorar os dispositivos pessoais: Monitorar os dispositivos que acessam a rede corporativa. Existem aplicações que isolam os dados, criando um abtiente corporativo fechado, dentro dos dispositivos do usuário. Estes aplicativos são fundamentais para o convívio em BYOD, pois além da separação do ambiente pessoal e corporativo, permite o monitoramento dos dispositivos e conteúdo acessado.

3.4.2 Cuidados com a rede *Wireless*

Assim como os demais ambientes, empresas que transmitem dados utilizando majoritariamente a rede WI-FI, devem adotar algumas medidas cautelares especiais. Quanto maior o número de dispositivos com acesso à internet presentes no ambiente, maiores serão as interferências na medida em que estes dispositivos transmitem dados (JÚNIOR, 2013). Destarte, deve haver um controle no ambiente *wireless* que tem de ser utilizado afim de evitar interferências, evitando que equipamentos concorram na mesma frequência.

Segundo Júnior (2013), a maioria dos equipamentos atualmente operam na faixa de 2,4GHz, sendo os mais utilizados. De acordo com o autor, equipamentos que possuem *wireless* geralmente possuem uma variação de frequência que vai de 2,4 GHz até 5GHz (figura 2).

Figura 2 - Distribuição de canais *wireless* 2,4 GHz no Brasil



Fonte: (JÚNIOR, 2013)

Todavia, esta frequência pode variar de local para local. Perini (2017) aponta que no Brasil, a faixa de frequência disponível para equipamentos *wireless* é de 2,412GHz até 2,472GHz, ou dos canais 1 ao 13. Segundo o autor supracitado, é

sugerido que as empresas optem por preferir canais distantes com o objetivo de evitar interferências, como o canal 1, 6 e 11. Além de tudo o que foi exposto, também é necessário levar em consideração que o ambiente *wireless* requer vigilância ativa.

De acordo com Perini (2018), o monitoramento é de extrema utilidade para que a empresa possa traçar uma linha de uso, capacidade dos equipamentos e consumo dos recursos. Alguns equipamentos que possuem *wireless* já possuem aplicações nativas que realizam este controle, alocando as frequências para equipamentos conhecidos e alterando os AP's em uma planta.

Contudo, o controle irá depender das necessidades da empresa, do seu fluxo de dados e dos equipamentos utilizados para o controle. De acordo com Júnior (2013), existem equipamentos que possuem funções extras, isto é, que além de detectar as melhores frequências, também detectam os tipos de pontos de acessos não autorizados, incluindo até mesmo *hotspots* móveis e soft APs que podem estar localizados nas áreas da empresa. Segundo o autor supracitado, existem diversos equipamentos no mercado que podem ajudar a empresa a realizar este tipo de controle.

Através deste controle, a empresa pode, por exemplo, detectar ou bloquear de maneira quase imediata quaisquer dispositivos móveis que tentem se conectar à rede sem autorização expressa.

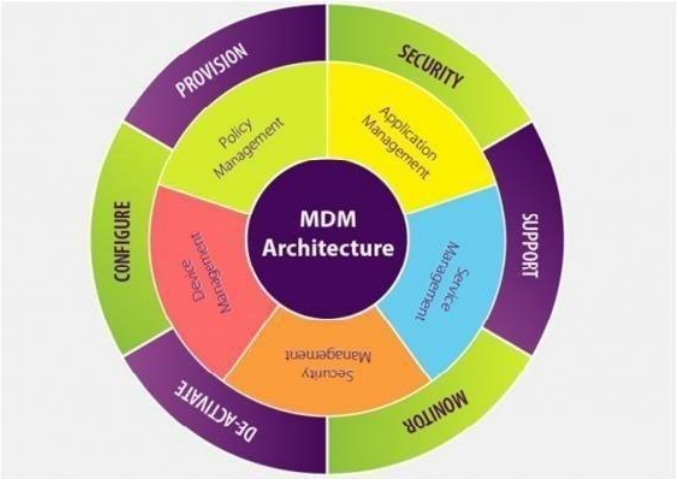
a) *Mobile Device Management* para dispositivos móveis em redes *Wireless*

Para o controle de dispositivos móveis em redes wireless, as ferramentas de MDM são utilizadas determinando quais usuários podem acessar qual tipo de conteúdo na rede, criando perfis customizáveis de acesso. A partir disso, as ferramentas de MDM (também conhecidas como ferramentas de gerenciamento do dispositivo móvel) possuem a finalidade de proteger o ambiente corporativo contra possíveis acessos não autorizados realizados através de dispositivos móveis.

Para que isto seja possível, o MDM se utiliza de filtros e registros dos acessos que foram realizados no ambiente corporativo. A partir destes registros, os administradores do sistema podem analisar e averiguar a entrada de qualquer dispositivo no ambiente corporativo. De acordo com Júnior (2013), alguns métodos de MDM utilizados podem até mesmo desligar o dispositivo instantaneamente ou apagar os dados baixados pelo usuário. O desenvolvedor de aplicações para dispositivos

móveis XCube Labs aponta que a MDM cria um ambiente de monitoramento altamente confiável, conforme apontado pela figura 3:

Figura 3 - Modelo de estrutura MDM



Fonte: (XCUBE LABS, 2013)

Todavia, a interferência física do MDM nos dispositivos móveis em alguns casos podem ferir políticas de ética, causando problemas desagradáveis na empresa. Caso haja algum acidente ou mal entendido, o usuário poderá ter o seu dispositivo formatado. Assim, embora o MDM seja um método eficaz, são necessárias algumas barreiras e entraves para que a proteção excessiva não cause irritação ou dissabores no ambiente corporativo (ESECURITY PLANET, 2013).

3.4.3 Divisão das medidas em diferentes níveis organizacionais

Existem diferentes soluções de segurança para BYOD em várias organizações que lidam apenas com domínios específicos em companhias. O modelo de política de segurança multinível em BYOD foi projetado para incluir as políticas necessárias para implementar a tecnologia BYOD de forma eficaz, sem comprometer a produtividade. A Figura 4 mostra a política de segurança multinível em BYOD. A política de segurança multinível é composta por três níveis - nível organizacional, nível de aplicativo e nível de políticas de dispositivo.

Figura 4 - Política de segurança multinível em BYOD

Fonte: (VIGNESH E ASHA, 2015)

a) Nível Organizacional

A organização deve considerar este nível antes de cadastrar um funcionário na política BYOD. As políticas de nível organizacional são uma lista de verificação antes de implementar o BYOD na organização. Um acordo recomendado: esclarecer a responsabilidade pelo suporte, manutenção e custos do dispositivo; certificar-se de que os usuários são responsáveis por fazer o backup de seus dados pessoais; os funcionários devem remover aplicativos no dispositivo a pedido da organização; O funcionário não deve usar os dispositivos com acesso root; e explicar as consequências para quaisquer violações à política.

O controle de acesso deve ser restrito ao funcionário com base em sua classe e descrição de cargo. A biometria é o mecanismo utilizado para registrar os dispositivos; os dispositivos não registrados não terão acesso às informações da rede da empresa. Todos os funcionários da organização não precisam trazer seus dispositivos pessoais para o trabalho. Esta parte fornece alguns perfis sugeridos que podem ser usados para classificar os funcionários (VIGNESH E ASHA, 2015).

1. Usuário padrão: o Usuário Padrão seria um funcionário básico que pode estar com a organização por um período mínimo de tempo e entende os fundamentos de segurança conforme definido por uma organização no processo de treinamento. Este funcionário estaria sujeito a trazer seu dispositivo para o trabalho e obter acesso à rede da empresa. A empresa pode limitar o acesso fora das instalações da empresa (VIGNESH E ASHA, 2015).

2. Usuário avançado: O usuário avançado é um funcionário de confiança o qual é permitido que o dispositivo seja usado no local de trabalho e em casa. O funcionário pode acessar as informações da empresa nas redes públicas, mas os dados confidenciais são negados a este usuário. É permitido ao seu dispositivo acesso semelhante em casa e no trabalho em termos de capacidades e privilégios (VIGNESH E ASHA, 2015).

3. Usuário profissional: Um usuário profissional é aquele que possui conhecimento avançado de segurança e é empregado altamente confiável.
Um administrador de redes ou o chefe da empresa se enquadram nesta categoria. Eles têm privilégios no acesso de qualquer informação da rede doméstica ou de rede não confiável na empresa. VPN e serviços em nuvem são usados para acessar informações confidenciais da empresa. O dispositivo deste usuário deve ser monitorado mais de perto por causa de seu alto privilégio (VIGNESH E ASHA, 2015).

4. Usuário convidado: o usuário convidado é um novo usuário da rede. Seus dispositivos não terão nenhum acesso à rede da organização usando seu dispositivo até que seja registrado na rede da empresa. O dispositivo não pode ser usado para acessar as informações da empresa até que o ispositivo tenha suas impressões digitais e seja verificado (VIGNESH E ASHA, 2015).

b) Nível de Aplicação

Este nível fornece segurança na forma de aplicativos móveis. Os smartphones são monitorados por aplicativos para ajudar o usuário a proteger os dispositivos. Esses aplicativos são conhecidos como Gerenciamento de Dispositivos Móveis (Mobile Device Management – MDM) (VIGNESH E ASHA, 2015).

Existem muitos fornecedores como AirWatch, Codeproof, Dell e Lookout que fornecem esses aplicativos. A abordagem de segurança do MDM é baseada em três ações básicas: controlar, monitorar e proteger. O servidor da empresa pode ser configurado e acessado a partir desses aplicativos (VIGNESH E ASHA, 2015).

O Gerenciamento de Dispositivos Móveis suporta o controle total do dispositivo como bloqueio, controle, conexão SSL com o servidor, limpeza remota, sirene, sinalização e backup de dados pessoais e aplica essas políticas em todos os dispositivos móveis. Gerenciamento de Aplicativos Móveis (Mobile Application Management – MAM), semelhante ao Gerenciamento de Dispositivos Móveis, é usado para controlar aplicativos específicos no dispositivo (VIGNESH E ASHA, 2015).

Os aplicativos monitorados são os corporativos que podem ser monitorados de perto e bloqueados. O MAM não é confiável, pois não fornece proteção completa para os dispositivos móveis. O MDM deve incluir o Gerenciamento de Conteúdo Móvel (Mobile Content Management – MCM), que é o mais importante ao lidar com informações confidenciais nos dispositivos. Os aplicativos monitorados são os

aplicativos corporativos que podem ser monitorados de perto e bloqueados. O MCM é usado para proteger os dados presentes nos smartphones, tablets e PDA'S. Os dados podem ser criptografados e armazenados no dispositivo. Se o dispositivo for roubado, os dados não podem ser recuperados. Com base na localização o bloqueio pode ser aplicado usando GPS (VIGNESH E ASHA, 2015).

Os dados podem ser descriptografados e acessados apenas em um ponto geográfico específico, como no local de trabalho e em casa. A verificação em duas etapas pode ser feita para acessar os dados. Primeira etapa para solicitar uma senha e segunda etapa para solicitar um número de token enviado ao número do celular de propriedade do usuário. Isso aumentará o segurança e diminuirá o número de problemas de propriedade (VIGNESH E ASHA, 2015).

Vignesh e Asha (2015) afirmam que deve haver um software de criptografia externa para criptografar o cartão de memória externo. Sempre que um usuário instala um aplicativo do *marketplace* ou app store, o aplicativo solicita permissão para acessar alguns recursos no celular, como:

- Detalhes da conta;
- Informação do aplicativo;
- Telefonemas;
- Comunicação de rede;
- Configurações de sincronização;
- Ferramentas do sistema;
- Localização;
- Câmera;
- Favoritos e histórico da web;
- Armazenamento.

As credenciais acima são confidenciais e alguns aplicativos solicitam acesso a essas credenciais, o que torna o dispositivo altamente vulnerável a ataques e os detalhes sobre o dispositivo podem vazar sem o conhecimento do usuário. O MDM deve monitorar e restringir o aplicativo a ser instalado. Esses aplicativos podem ser malwares e os dados podem ser roubados dos dispositivos por meio da rede. O MDM deve avisar o usuário antes de instalar tais aplicativos nos dispositivos móveis (VIGNESH E ASHA, 2015).

c) Nível de Dispositivo

A maioria das organizações deixa as políticas de segurança de nível do dispositivo e presume que depende do proprietário e do fabricante do dispositivo. Algumas políticas de nível de dispositivo são: autoridade de certificação, criptografia de dados, multiusuário e problema de enraizamento (VIGNESH E ASHA, 2015).

Agora, todo smartphone vem com credenciais de autoridade de certificações confiáveis pré-instaladas como American online, COMODO, thawte, verisign, VISA e muitas outras. Essas credenciais estavam ocultas em versões anteriores do smartphone. No smartphone mais recente, essas credenciais podem ser gerenciadas. O usuário pode adicionar novos certificados e remover certificados existentes. Remover um certificado fará com que o usuário trabalhe online em um ambiente de rede não confiável. Há chances de adicionar uma autoridade de certificação falsa aos smartphones que obtêm os detalhes do usuário e ocorre violação de dados. Se o certificado for hackeado, há chances de acessar o dispositivo e se a empresa usa o mesmo certificado, então o hacker pode obter acesso ao servidor (VIGNESH E ASHA, 2015).

Portanto, o dispositivo deve monitorar as credenciais. O smartphone mais recente vem com aplicativo de criptografia embutido. Isso criptografará os dados como contas, configurações e aplicativos. Mas o usuário não se preocupa em ver essa opção e também leva várias horas para concluir com base na capacidade de armazenamento do dispositivo (VIGNESH E ASHA, 2015).

Existem opções disponíveis para criptografar o cartão SD inserido em alguns smartphones. Os dispositivos de desbloqueio ou root passam despercebidos em várias organizações. *Jailbreak* ou enraizamento referem-se ao ganho de privilégio administrativo nos smartphones. Semelhante ao Linux, os usuários root são administradores e têm privilégio para modificar o sistema operacional e instalar qualquer aplicativo no sistema. Se os smartphones estiverem enraizados, então, o usuário pode instalar aplicativos não autorizados que adulteram ou vazam dados confidenciais no dispositivo (VIGNESH E ASHA, 2015).

Em geral, iphones e telefones Android têm acesso root. O rooting é realizado legalmente na Austrália, EUA e Reino Unido. A organização deve evitar que os dispositivos com root sejam usados na empresa como parte do BYOD (VIGNESH E ASHA, 2015).

4 *MICROSOFT INTUNE* – SOLUCÃO COMPLETA DE MDM E MAM

Conforme mencionado anteriormente, a adoção de uma solução direcionada com um único método de gerenciamento, monitoramento e controle pode aumentar muitos as probabilidades da ocorrência de incidentes de segurança, uma vez que, ainda existirão “pontos cegos” na administração destes dispositivos, para minimizar esses gargalhos, o uso de uma solução que contemple o Gerenciamento do Dispositivo Móvel (MDM) e de Aplicações (MAM) dos dispositivos. Dentre as possibilidades de mercado, o *Microsoft Intune* se apresenta como uma solução bem estruturada, uma vez que agrega os dois modos de gestão dos dispositivos móveis em uma gestão centralizada, contudo, com possiblidades de administração remota.

De acordo com a documentação do software disponível no site Microsoft (MICROSOFT, 2020), “O Intune é um serviço baseado em nuvem que ajuda a habilitar sua força de trabalho a ser produtiva enquanto mantém os dados corporativos protegidos. Conheça os conceitos básicos de planejamento, migração e configuração do Intune.”

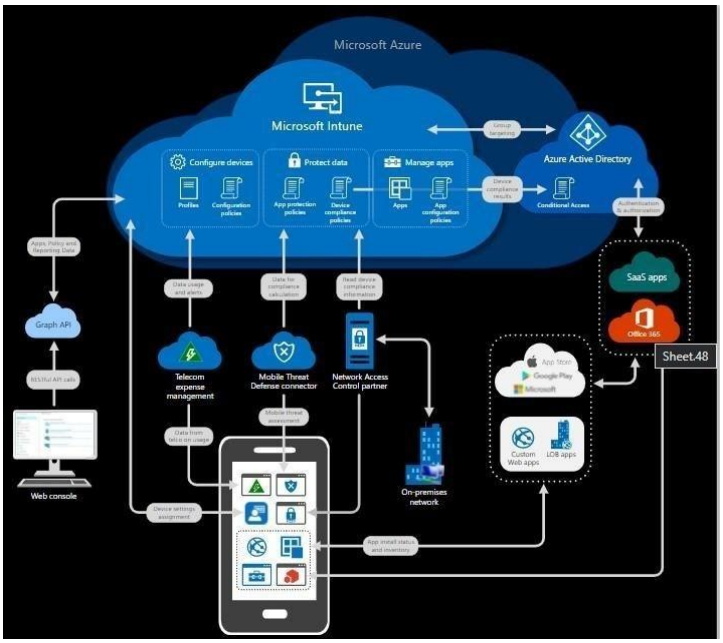
> O Microsoft Intune é um serviço baseado em nuvem que se concentra no MDM (gerenciamento de dispositivo móvel) e no MAM (gerenciamento de aplicativo móvel). Você controla como os dispositivos da sua organização são usados, incluindo telefones celulares, tablets e laptops. Você também pode configurar políticas específicas para controlar aplicativos. Por exemplo, você pode impedir que e-mails sejam enviados para pessoas de fora da sua organização. O Intune também permite que as pessoas em sua organização usem dispositivos pessoais para escola ou trabalho. Em dispositivos pessoais, o Intune ajuda a garantir que os dados da sua organização permaneçam protegidos e pode isolar os dados da organização de dados pessoais. (Microsoft Intune, 2020).

A ferramenta é integrada a diversas outras soluções de conectividade da própria Microsoft consolidadas no mercado conforme Figura 5, e com essa integração, permite ofertar outras possibilidades de aplicações para compor o suíte de softwares a serem utilizados na organização em questão.

> “O Intune faz parte do pacote EMS (Enterprise Mobility + Security) da Microsoft. O Intune integra-se com o Azure AD (Azure Active Directory) para controlar quem tem acesso e o que eles podem acessar. Ele também se integra à Proteção de Informações do Azure para oferecer proteção de dados. E ele pode ser usado com o pacote de produtos do Microsoft 365. Por

exemplo, você pode implantar o Microsoft Teams, o OneNote e outros aplicativos do Microsoft 365 em dispositivos. Esse recurso permite que as pessoas em sua organização sejam produtivas em todos os dispositivos, mantendo as informações da organização protegidas com as políticas que você criou.” (Microsoft Intune, 2020).

Figura 5 – Arquitetura do Intune



Fonte: *Docs.Microsoft*

Segundo a documentação do Servido, a integração da ferramenta permite os seguintes tipos de gerenciamento de plataforma com o Intune:

- Escolha estar 100% na nuvem com o Intune ou ser *Co gerenciado* com o *Configuration Manager* e o Intune.
- Defina regras e configurações em dispositivos pessoais e de propriedade da organização para acessar dados e redes.
- Implante e autentique aplicativos em dispositivos locais e móveis.
- Proteja as informações da empresa controlando a maneira como os usuários acessam e compartilham informações.
- Os dispositivos e aplicativos devem atender aos requisitos de segurança.

4.1 Gerenciamento de dispositivos no Intune

Assim como toda ferramenta de gerenciamento de dispositivos, o Intune tem suas particularidades, principalmente pela integração mencionada anteriormente.

> No Intune, você gerencia os dispositivos usando uma abordagem adequada para você. Para dispositivos de propriedade da organização, convém ter controle total sobre os dispositivos, incluindo configurações, recursos e segurança. Nessa abordagem, os dispositivos e os usuários desses dispositivos "inscrevem-se" no Intune. Depois de inscritos, eles recebem suas regras e configurações por meio de políticas configuradas no Intune. Por exemplo, você pode definir os requisitos de senha e PIN, criar uma conexão VPN, configurar a proteção contra ameaças e muito mais. (Microsoft Intune, 2020).

Segundo o documento, quando a aplicação esta efetivamente direcionada ao BYOD, ela permite ao usuário não acessar todos os recursos que estão direcionados a organização, contudo, por utilizar recursos de terceiros, a ferramenta exige a implementação da autenticação multifator, trazendo mais garantias do cumprimentas das políticas de segurança da empresa.

Conforme documentação do Intunes, os administradores podem:

- Ver os dispositivos registrados e obter um inventário dos dispositivos que acessam os recursos da organização.
- Configurar os dispositivos para que eles atendam aos padrões de segurança e integridade. Por exemplo, você provavelmente desejará bloquear dispositivos com *jailbreak*.
- Envie certificados por *push* para os dispositivos para que os usuários possam facilmente acessar sua rede Wi-Fi ou usar uma VPN para se conectar à sua rede.
- Conferir relatórios sobre usuários e dispositivos que estão em conformidade ou não.
- Remover os dados da organização de um dispositivo caso ele seja perdido, roubado ou não seja mais usado.

4.2 Gerenciamento de aplicativos no Intune

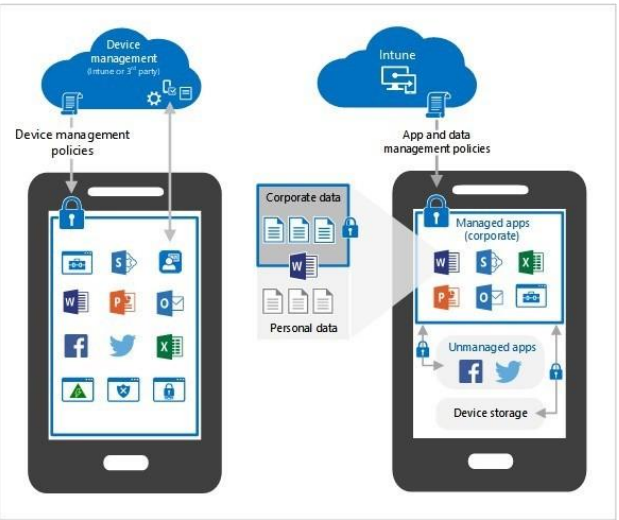
Uma solução que consiga fazer o gerenciamento de aplicativo e do dispositivo, tem mais efetividade na garantia de efetivação das políticas de segurança da organização, e para ter essa ferramenta de forma completa, o gerenciamento de aplicativos já é uma predefinição do serviço, conforme Figura 6.

Segundo a documentação do software, “O MAM no Intune foi projetado para proteger os dados da organização no nível do aplicativo, inclusive aplicativos personalizados e aplicativos da loja. O gerenciamento de aplicativos pode ser usado em dispositivos pessoais e de propriedade da organização”.

Após a ativação do dispositivo, os administradores podem:

- Adicionar e atribuir aplicativos móveis a grupos de usuários, inclusive usuários em grupos específicos, dispositivos em grupos específicos e muito mais.
- Configurar aplicativos para iniciar ou executar com configurações específicas habilitadas e atualizar os aplicativos existentes que já estão no dispositivo.
- Conferir relatórios sobre quais aplicativos são usados e acompanhar o uso deles.
- Fazer um apagamento seletivo removendo somente os dados da organização dos aplicativos.

Figura 6 – Gestão de aplicativos no Intune



Fonte: *Docs.Microsoft*

5 CONSIDERAÇÕES FINAIS

A partir do crescimento exponencial e da propagação vertiginosa dos dispositivos móveis no ambiente empresarial, aliados aos novos modelos de destes, cada vez mais acessíveis, é inevitável a utilização no ambiente empresarial por seus usuários com uso de seus próprios dispositivos no ambiente de trabalho, sendo este um dos principais pressupostos do *BYOD*.

Entretanto, a adoção deste modelo, perpassa por aspectos positivos e negativos inicialmente vislumbrados em sua implementação, tal como qualquer nova solução, a adequação é necessária para que se alcance a produtividade esperada. Com uma grande quantidade de dispositivos pessoais no ambiente de trabalho, a empresa tem de lidar com um maior tráfego de informações em suas redes, afetando tanto o desempenho da mesma quanto a segurança dos dados críticos que são um dos principais patrimônios ativos de qualquer ambiente corporativo.

A partir do que foi apontado, este estudo expôs os conceitos acerca do *BYOD* e os principais métodos que as empresas podem utilizar para salvaguardar as suas informações ao mesmo tempo em que ela consegue manter com eficácia do método.

Como aspecto principal, a importância das políticas de segurança dentro do ambiente empresarial, demonstrando aos funcionários quais são os limites que eles possuem na utilização de dispositivos móveis para que não haja comprometimento da segurança das informações nem no seu rendimento profissional. Para isto, é necessário que o ambiente corporativo possua administradores e profissionais preparados para gerir todo este sistema, já que o *BYOD* não se trata exatamente de uma tecnologia, mas sim de um modelo de operação.

Existem no mercado diversas solução que podem se caracterizar como *BYOD*, contudo, a definição do planejamento total, deve levar em consideração todos os aspectos relacionados à boa gestão de segurança da informação e da produtividade. O Microsoft Intune, foi uma solução completa apresentada para exemplificar todos os lineares necessários de serem abordados na administração destes usuários e seus dispositivos pessoais.

Conclui-se neste estudo, que a adoção do *BYOD* é uma excelente alternativa, uma vez que, os custos operacionais com infraestrutura computacional, podem diminuir, todavia, os investimentos devem ser redirecionados aos demais aspectos de gestão tecnológica e da informação da organização, trazendo assim, também um

ponto a favor deste modelo, uma vez que a proteção dos ativos se tornam a prioridade dos administradores e com isso, menos incidentes de segurança podem ocorrer nesta infraestrutura. A necessidade de atualização torna-se constante por parte da equipe de TI, uma vez que, as tecnologias devem acompanhar a evolução dos dispositivos dos funcionários. São várias evidencias positivas que tornam a adoção do BYOD uma eficiente solução empresarial.

REFERÊNCIAS

ANATEL. **Relatório de Acompanhamento de Setor de Telecomunicações**, 2021.Disponível em: <https://sei.anatel.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_exter na.php>. Acesso em 12 de junho. 2021.

CIO. **Proteção de dados em dispositivos móveis preocupa mais do que ciberataques**, 2016. Disponível em: <http://cio.com.br/noticias/2016/11/25/protecao- de-dados-emdispositivos-moveis-procupa-mais-do-que-ciberataques/> Acesso em: 14 de jun. 2021.

COMETTI, Mariana Beltran. **Políticas de segurança da informação para BYOD**.Revista Tecnológica da Fatec Americana. 2016.

COMPUTER WORLD. **3,8 milhões de smartphones são vendidos no mundo diariamente**, 2016. Disponível em: < http://computerworld.com.br/38-milhoes-desmartphones-sao-vendidos-nomundo-diariamente>. Acesso em: 17 de jun. 2021.

DELANEY, Darragh. **Remote access technologies in a BYOD era**, 2012. Disponível em:<http://www.computerworld.com/article/2472058/infrastructuremanagement/remo te-access-technologies-in-a-byod-era.html>. Acesso em: 15 de jun. 2021.

EARLS, Alan. **Closing the gate: Data leak prevention**, 2015. Disponível em:< https://www.scmagazine.com/closing-the-gate-data-leak-prevention/article/536721/>. Acesso em: 15 de jun. 2021.

ESECURITY PLANET. **BYODFuels NACComeback**. Disponível em: <http://www.esecurityplanet.com/network-security/byod-fuels-nac-comeback.html> Acesso em 22 de jun. 2021.

ISACA. **Cybersecurity Fundamentals Glossary**, p. 1-35, 2016. Disponível em: <https://www.isaca.org/Journal/archives/2012/Volume-1/Documents/12v1-DatabaseBackup.pdf>. Acesso em: 17 de jun. 2021.

JOHNSON, Kevin; DELAGRANGE, Tony. **SANS Survey on Mobility/BYOD Security Policies and Practices**. 2013. Disponível em: <https://www.yumpu.com/en/document/read/15705161/sans-survey-on-mobility-byodsecurity-policies-and-practices>. Acesso em: 17 de jun. 2021.

JUNIOR, Rodrigo Ramiro Muniz. **Desafios de BYOD em redes emergentes**. Universidade Tecnológica Federal do Paraná. Monografia. 2013.

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos metodologia científica**. 4.ed.São Paulo: Atlas, 2001.

MALATHY S.; KANTHA P. Application of Mobile Technologies to Libraries. **Journalof Library & Information Technology**, v. 33, n. 5, p. 361-366, set. 2013.

MICROSOFT. **Documentação Microsoft Intune**, 2020. Disponível em https://docs.microsoft.com/pt-br/mem/intune/fundamentals/. Acesso em 12 Junho de2021.

MORROW, Bill. **BYOD security challenges**: control and protect your most sensitive data, 2012. Disponível em:< http://ac.els-cdn.com/S1353485812701113/1-s2.0-S1353485812701113-main.pdf?_tid=c89b8a76-13b2-11e7-b676-00000aacb362&acdnat=1490704605_ab0fb0842c0b93960949633cf8afd270>. Acesso em: 12 de jun. 2021.

PELTIER, THOMAS. **Information Security Policies, Procedures, and Standards – Guideline for effective Information Security Management**, Florida, Auerbach, 2001.

PERINI, Vinícius Lahm. **Integração de Ferramentas de Administração e Segurança BYOD**. Universidade Caxias do Sul. Monografia. 2017.

SANTOS, Wagner Dobzinski. **Políticas de uso e segurança da informação**: um estudo sobre aplicação BYOD - Bring Your Own Device. Universidade TecnológicaFederal do Paraná. Monografia. 2017.

SOMMERFELD, Rafael. **Como sobreviver ao paradoxo da Shadow IT x TI Convencional**, 2015. Disponível em: < http://computerworld.com.br/como-sobreviverao-paradoxo-da-shadow-it-x-ti-convencional> Acesso em: 14 de jun. 2021.

SYNNEX WESTCON. **Según El Informe De Phishme El 93% De Los Emails Phishing Son Ransomwares**. 2016. Disponível em: < https://digital.la.synnex.com/segun-elinforme-de-phishme-el-93-de-los-emails-phishing-son-ransomwares>. Acesso em: 17 de jun. 2021.

TRAXLER, John. **Students and mobile devices. ALT-J Research in Learning Technology**, v. 18, n. 2, p. 149-160, jul. 2010.

TAURION, Cezar. **Cloud Computing**: computação em nuvem: transformando o mundo da tecnologia da informação. Editora Brasport: Rio de Janeiro, Brasil. 2009.

TELTEC SOLUTIONS. **BYOD e consumerização**: o que são e como utilizar. 2013. Disponível em < http://blog.teltecnetworks.com.br/category/byod/> Acesso em 21 dejun. 2021.

TORRES, Catarina; CARVALHO, Hugo; SILVA, Pedro. **Segurança dos Sistemas de Informação: Gestão Estratégica de Segurança Empresarial**. Editora CentroAtlântico: Lisboa, Portugal. 2003.

THOMSON, Garret. **BYOD**: Enabling the chaos. Network Security. 2012. Disponível em: <http://ac.els-cdn.com/S1353485812700132/1-s2.0-S1353485812700132main.pdf?_tid=92dc444c-1930-11e7b49f00000aab0f02&acdnat=1491308387_1def13472b9f5763bbf3d839be478be c>. Acesso em: 12 de jun. 2021.

VERGARA, Sylvia C. **Projetos e relatórios de pesquisa em administração**. 3.ed.Rio de Janeiro: Atlas, 2000.

VIGNESH, U; ASHA, S. **Modifying security policies towards BYOD**. 2nd International Symposium on Big Data and Cloud Computing. 2015.

[X]CUBE LABS. **Mobile Device Management enable manage and secure your mobile environment**. Disponível em: < http://www.xcubelabs.com/blog/mobile-devicemanagement-enable-manage-and-secure-your-mobile-environment/> Acessoem 22 de jun. 2021.

ZONG, Bu. **From smartphones to iPad**: Power users' disposition toward mobile media devices. Computers in Human Behavior, n. 29, p. 1742-1748, 2013.