UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM TECNOLOGIA
CURSO DE ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO
DE SERVIDORES E EQUIPAMENTOS DE REDE

RODRIGO RAMIRO MUNIZ JUNIOR

DESAFIOS DE BYOD EM REDES EMERGENTES

MONOGRAFIA

CURITIBA
2013

RODRIGO RAMIRO MUNIZ JUNIOR

DESAFIOS DE BYOD EM REDES EMERGENTES

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Configuração e Gerenciamento de servidores e equipamentos de rede, do Programa de Pós-Graduação em Tecnologia. Universidade Tecnológica Federal do Paraná. Área de Concentração: Redes de Computadores

Orientador: Prof. MSc. Fabiano Scriptore de Carvalho

CURITIBA

2013

RESUMO

MUNIZ JUNIOR, Rodrigo Ramiro. **Desafios de BYOD em redes emergentes**. 2013. XX f. Monografia (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

A presente monografia aborda um estudo sobre BYOD (Bring your own device) e levanta fatores a serem implementados na rede, como equipamentos, capacidade e funcionalidade diante de novos dipositivos fora do domínio. Apresenta também questões de segurança, como a interferência nas redes e espectro, segurança da informação e os riscos que estes dispositivos podem trazer. A monografia inicia com a apresentação dos assuntos e vai abordando os pontos apresentados, explorando os mais importantes a serem levantados para a aceitação destes dispositivos sem o comprometimento da estrutura atual e informação confidencial.

Palavras-chave: Redes. BYOD. Segurança

ABSTRACT

MUNIZ JUNIOR, Rodrigo Ramiro. **BYOD Challenges in Emerging Networks**. 2013. XX f. Monograph (Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes). Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

This monograph discusses a study on BYOD (Bring your own device) and contextualizes factors to be implemented on the network, such as equipment, capacity and functionality face new dipositivos outside the domain. It also presents security issues such as interference and spectrum networks, information security and the risks these devices can bring. This document paper begins with the presentation of the issues and will addressing the points presented, exploring the most important to be surveyed for the acceptance of these devices without compromising the current structure and confidential information.

Keywords: Network. BYOD. Network security.

LISTA DE SIGLAS

ACL – Access Control List

AP – Access Point

APs – Access Points

BYOD – Bring Your Own Device

CTS – Clear do send

CSMA/CA - Carrier Sense Multiple Access with Collision Avoidance

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name System

EAP - Extensible Authentication Protocol

GHz – Giga Hertz

HTTP - Hypertext Transfer Protocol

IEEE - Institute of Electrical and Eletronics Engineers

IP – Internet Protocol

LAN – Local Area Network

MAC - Media Access Control

Mbps - Megabits por Segundo

MDM - Mobile Device Management

MIMO - Multiple-Input Multiple-Output

RFC - Request for Comments

RTS – Request to send

RADIUS - Remote Authentication Dial In User Service

TCP - Transmission Control Protocol

TCP/IP - Transmission Control Protocol over Internet Protocol

TI – Tecnologia da Informação

VLAN - Virtual Local Area Network

WLAN – Wireless Local Area Network

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. INTRODUÇÃO

BYOD, acrônimo de *Bring your own device* ou em português: traga seu próprio dispositivo, é tendência mundial para empresas e pessoas, que vem pegando de surpresa administradores de redes frente ao crescimento exponencial de dispositivos e novas políticas para redes de computadores.

O BYOD, que permite que os funcionários levem seus próprios dispositivos para o ambiente de trabalho, ainda não é uma realidade nas empresas brasileiras, mas tende a mudar em pouco tempo e os gestores de TI não conseguirão escapar desse movimento. O recado é da analista do Gartner Elia San Miguel, noticiado no site ComputerWorld. (COMPUTERWORLD, 2013).

Dispositivos móveis estão causando um grande impacto no ambiente de trabalho e nas redes de computadores. Ainda sob visão da analista do Garnter, percebe-se que as companhias não estão preparadas para esse processo de mudança, que exige adaptações específicas de infra-estrutura, segurança e adaptação pessoal.

1.1. TEMA

O alto consumo de dispositivos móveis como *tablets*, *smartphones* e *notebooks* pessoais, traz para o setor de Tecnologia da informação (TI) novos desafios no ambiente empresarial.

O BYOD se destaca entre os usuários, pois estes encontram em seus dispositivos, ambiente amigável e de seu controle. Além disto a capacidade de processamento destes dispositivos muitas vezes supera os equipamentos profissionais, o que agrada para a realização de tarefas.

Para ambientes empresariais, a implementação de programas direcionados ao BYOD é hoje umas das mudanças mais radicais para os setores de TI. A TI tradicional, acostumada a ter sob domínio o acesso a máquinas passa a fornecer acesso a um grande número de dispositivos, na qual não tem total controle.

Os desafios do BYOD incluem, além do aumento do número de dispositivos acessando a rede, problemas de capacidade de tráfego interno e externo, atualização de equipamentos e recursos humanos e também problemas de segurança de rede e segurança de informação.

Uma característica de dispositivos BYOD, é que estes são essencialmente móveis. Neste caso, em se tratando de estrutura de redes, o projeto e a política da rede *wireless* devem exigir cuidados especiais, desde a implantação da estrutura, abrangendo tanto políticas de segurança como políticas de controle.

1.2. PROBLEMAS E PREMISSAS

Dispositivos pessoais são em geral um risco a segurança de uma rede corporativa. Contudo, estes dispositivos tem uma característica em comum, a portablidade, e estão sendo levados para dentro de empresas.

É ineficaz remar contra a maré, o BYOD já esta acontecendo e vai ganhar cada vez mais espaço nas empresas. Quanto antes se entender e preparar este cenário, conhecendo as formas de gerenciar e controlar, mais rápido e com mais segurança será tratado. Administradores de redes de computadores devem entender as novas necessidades da rede.

Como vantagem, esta tendência é vista com bons olhos por parte dos colaboradores, e também pelas empresas, que consideram a economia de dinheiro, evitando compra desnecessária de *hardware* e *software*.

1.3. OBJETIVOS

1.3.1. Objetivo Geral

Apresentar os desafios que o BYOD está trazendo para as redes de computadores e discutir a respeito dos riscos, dificuldades e tecnologias envolvidas para atender a necessidade do BYOD e explorar a segurança da rede e falhas que podem fragilizar a estrutura não preparada para o ingresso volátil e randômico de dispositivos.

1.3.2. Objetivos Específicos

- Estudar os cenários atuais de BYOD, para compreender e explorar como o conceito está sendo aplicado para os usuários e para as redes de computadores. Levantar informações deste estudo como coleta de dados, em breve análise da tecnologia e estrutura de redes;
- Apresentar algumas visões dos cenários de BYOD para as redes de computadores, e exibir soluções básicas e simples com o intuito de ajudar técnicos e administradores de redes a reconfigurar a estrutura;
- Contribuir mostrando uma visão sobre soluções, de modo a tentar deixar claro os riscos inerentes ao processo de aceitação de dispositivos do BYOD.

1.4. JUSTIFICATIVA

Trabalhar em uma empresa de telecomunicações que desenvolve e comercializa produtos ativos de redes de computadores, entre eles, ponto de acesso *wireless*. Atuando junto com o desenvolvimento destes equipamentos, faz-se o acompanhamento do mercado, que fez enxergar a migração para redes móveis e o crescimento do BYOD.

Com o aumento da quantidade de dispositivos móveis, administradores de redes veem requisitando soluções mais corporativas e prontas para a gerência de BYOD. O que também exibe certa deficiência na administração das redes.

Umas das razões deve-se ao crescimento rápido dos dispositivos móveis, que pegou de surpresa alguns administradores. Outro motivo, não acreditar que BYOD precisa de soluções dedicadas. Com isto, administradores estão sentindo os impactos na rede, o que demonstra que as redes não estão preparadas para o crescimento rápido.

Este cenário exigiu o início de soluções mais profissionais. Após análise das redes que chegavam com problema, e desenvolvendo soluções que atendem a requisitos mínimos de capacidade, percebeu-se a necessidade de um estudo mais avançado sobre as necessidades para empresas.

1.5. PROCEDIMENTOS METODOLÓGICOS

A pesquisa bibliográfica será feita com o intuito de aprofundar o conhecimento e a realidade. Serão abordados alguns tópicos de acordo com os mais relevantes artigos encontrados.

A interpretação do material lido será utilizada como objeto de estudo para apresentar principais dificuldades e algumas soluções para os problemas gerados pelo uso de BYOD.

1.6. ESTRUTURA

A monografia é composta por 4 capítulos, sendo o capítulo 1, uma breve introdução do tema, do objetivo do trabalho a justificativa que motivou a escolha do assunto para o desenvolvimento do trabalho.

O referencial teórico é abordado no capítulo 2, apresentando o BYOD, suas vantagens e desvantagens. Questões de segurança são exploradas para mostrar riscos do uso de BYOD.

O capítulo 3 apresenta alguns modelos de boas práticas de configuração de equipamentos e modelos a seguir para configuração e manutenção de redes para atender a demanda BYOD, bem como mostra a necessidade de treinamento pessoal.

Concluindo, o capítulo 4 apresenta perspectivas de crescimento de BYOD, com algumas considerações a respeito do conceito, e da segurança a respeito da rede e do modelo.

2. REFERENCIAL TEÓRICO

O referencial teórico apresenta o conceito de BYOD, e descreve as vantagens e os riscos inerentes ao uso de dispositivos pessoais e móveis em um ambiente corporativo.

Os administradores aprenderam ao longo da carreira que ter o controle total dos dispositivos, desde servidores até os computadores de usuários, sob domínio do administrador é a opção mais segura e correta de administração.

A administração de redes deve ser feita desde o projeto até técnicas de manutenção, e dentro disto, assumir novas tecnologias e necessidades trazidas por usuários como um desafio constante. Em se falando de administração para o BYOD, a maneira mais fácil de proteger a rede é assumir que os dispositivos móveis acessem a empresa, para a criação de ambiente controlado.

Apesar de ter o maior impacto em empresas privadas, o BYOD está presente também em órgãos públicos, escolas, hospitais, etc.

A estrutura da rede, equipamentos ativos, requer políticas que aceitem estes dispositivos e evitem gargalos internos. Uma rede que está perto do limite com os dispositivos atuais, não aguentará nova demanda e aumentará as taxas de atraso e perda de pacotes por conta de estouros em *buffer* nos ativos da rede.

Segmentar os impactos para avaliação, em *uplink*, redes *wireless* e estrutura de rede é uma alternativa para monitorar e iniciar uma avaliação de riscos e necessidades.

2.1. Conceito de BYOD

A mobilidade de dispositivos mudou significativamente nos últimos anos, começando pelo *notebook* e atingindo telefones, *smartphones* e *tablets*. Estes dispositivos foram migrando para o ambiente corporativo, e ganhando valor pela aproximação do funcionário com escritórios, num ambiente relativamente controlado.

Os usuários, nos dias de hoje, se acostumaram com o acesso fornecido por seus dispositivos e estão levando estes dispositivos para o trabalho. De acordo com uma pesquisa realizada pela Fluke Networks, com a ascensão nas companhias do fenômeno BYOD, os técnicos de rede passaram a gastar 48% a 58% mais tempo com as redes WLAN e com problemas relacionados com os dispositivos emergentes. (INFORMATION MANAGEMENT, 2013)

Segundo recente pesquisa da Cisco (CISCO ISBG, 2012), o BYOD é um fenômeno global, e as empresas devem responder de forma pró ativa ao BYOD com melhores políticas a dispositivos móveis e estratégias de redução de custos.

Em uma conferência da IEEE em 2012, o artigo "Analyzing Consumerization - Should Enterprise Business Context Determine Session Policy?" apresentado mostrava alguns números da penetração de BYOD. A figura exibe um resumo destes números por tipo de dispositivo, sendo que cada usuário pode ter mais de um dispositivo:

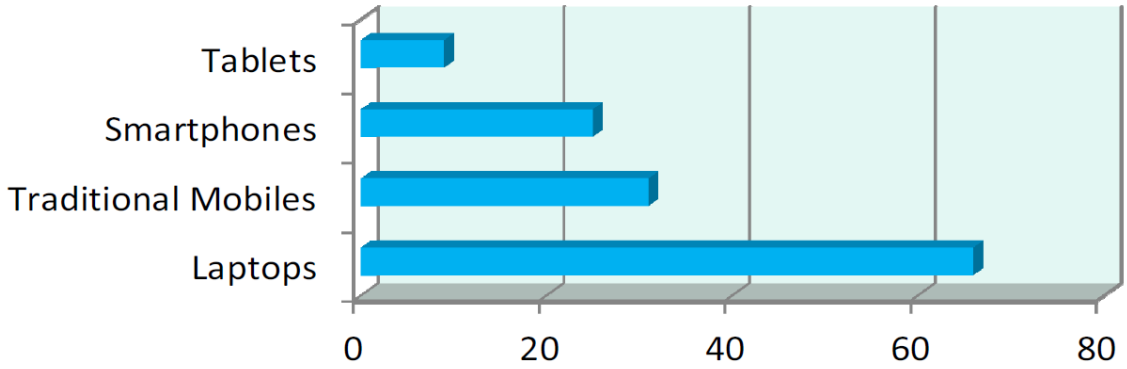

Figura 1 - Penetração de BYOD por dispositivo em %

Fonte: COPELAND, IEEE, 2012

A CISCO apresenta pesquisa (CISCO ISBG, 2012), que aponta que líderes de TI esperam que o número de dispositivos aumente da média de 2,3 por funcionário em 2012 para 2,8 em 2014, conforme mostrado na figura abaixo:

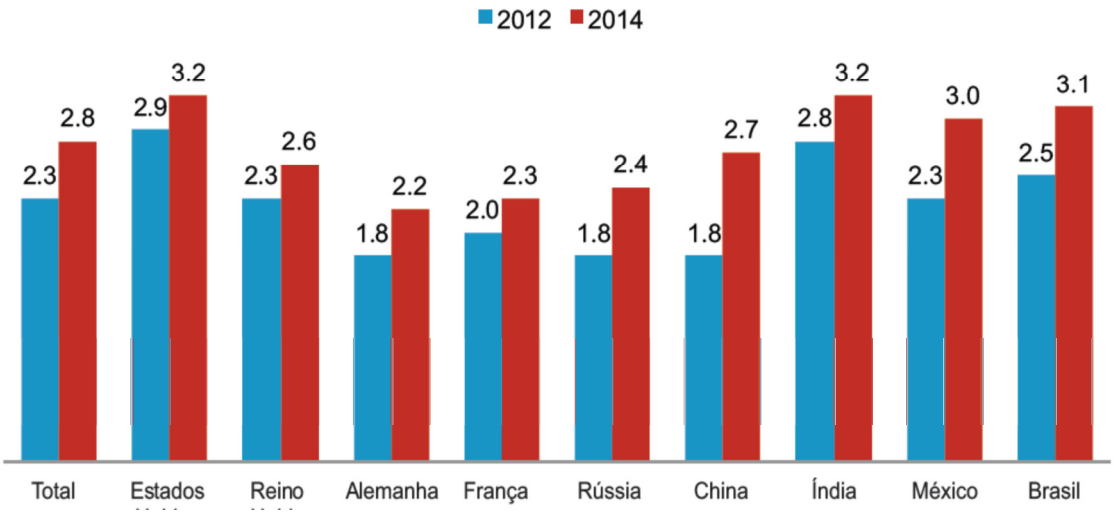

Figura 2 - Número médio de dispositivos conectados por profissional, 2012 e 2014.

Fonte: CISCO ISBG, 2012

2.2. Vantagens do uso

As vantagens de uso, em geral, são relacionadas ao lado social e rentabilidade da empresa, sendo identificados aumento de produtividade por parte dos funcionários, que trabalham em um ambiente conhecido e com permissões administrativas. Redução de custos para a empresa, pois o equipamento que o funcionário utiliza não é contabilizado no investimento e também, satisfação no trabalho.

Neste documento será abordado a parte técnica, deixando de lado questões relacionadas à administração financeira e conceitos sociais. Contudo, vale ressaltar que dentre os profissionais de TI que já enxergam o BYOD, no Brasil, 76% veem esta tendência como positiva.

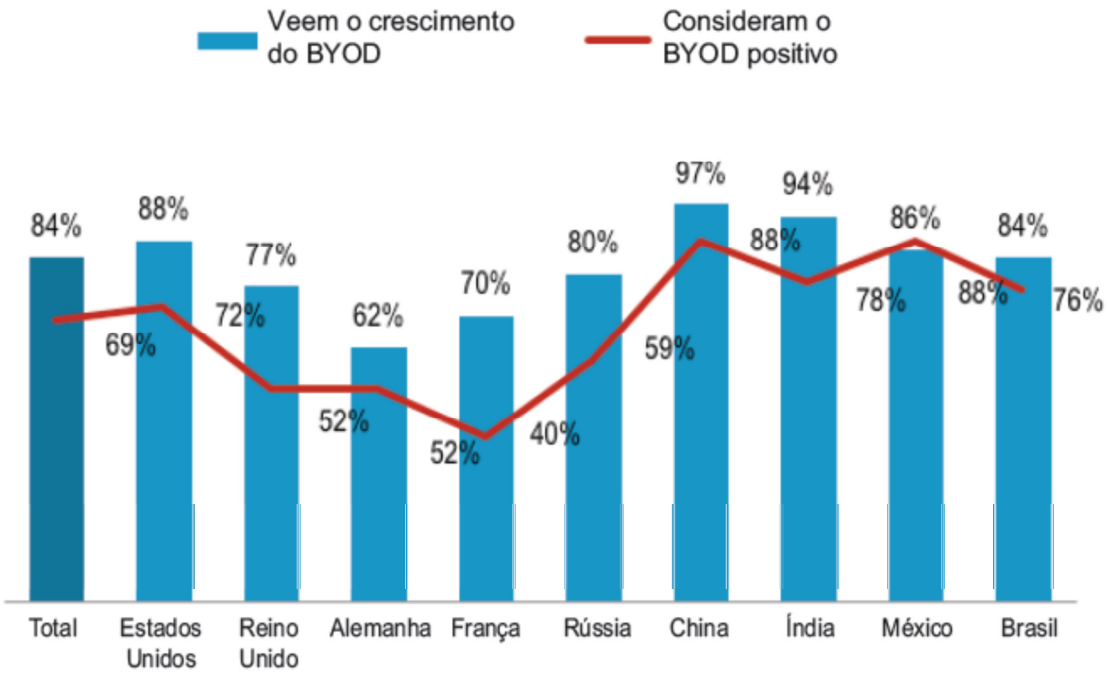

Figura 3 - Percentual de líderes de TI que consideram a tendência positiva

Fonte: CISCO ISBG, 2012

2.3. Desvantagens do uso

Embora os benefícios da mobilidade sejam claros e atrativos, também há desvantagens nessa tendência. Diversidade de dispositivos e sistemas operacionais e acréscimo de várias plataformas a rede, exigem suporte e escalabilidade.

Com a escalabilidade, os requisitos para políticas de segurança relacionadas à autenticação, autorização e provisionamento devem ser analisados de modo essencial.

Hoje, o mercado de TI oferece tecnologia para estabelecer mecanismos de controle de acesso capazes de identificar o acesso à rede, tipo de dispositivo, computador e onde é utilizado.

Muitos destes acessos são realizados através de redes *wireless*, onde são necessárias controladoras *wireless*, para gerência dos pontos de acesso sem fio e específicos para o ambiente de rádio frequência. Além destes controles, devem ser avaliadas também alternativas de *Mobile Device Management* (MDM).

2.4. Problemas de segurança de rede

Uma empresa ou organização deve ter como costume a homologação dos dispositivos de rede que serão utilizados. Esta homologação deve atender requisitos mínimos, para que facilite a administração e configuração das máquinas e a prestação de serviços.

Quando os usuários utilizam seus próprios dispositivos e aplicativos, isso implica em possíveis custos para a empresa. Um deles é o aumento na largura de banda que muitos desses aplicativos exigem. A combinação de mais dispositivos na rede e aplicativos não homologados pode criar gargalos, a não ser que os departamentos de TI estejam atentos aos planejamentos dos recursos e gerenciamento de rede.

Imaginar que usuários irão utilizar seus próprios dispositivos gera problemas imediatos de confidencialidade dos dados da organização, ao entrar e sair de dentro das paredes e controle de uma empresa, o dispositivo pode virar um *backdoor*, conter vírus e outras pragas que podem inundar uma rede de informação desnessária, ou permitir acesso remoto a um dispositivo internamente conectado.

Vírus podem, por exemplo, inundar tabelas MAC e *buffer* de *switches* e roteadores com tempestades de *broadcast*, o que irá reduzir a performance da rede. Mas este problema pode também ser causado pelas diversas aplicações que podem estar instaladas no dispositivo.

Tratando das aplicações, as do usuário podem, por exemplo, não ser compatível com o *software* da organização, devido a diversidade de versões. As diversas aplicações podem gerar tráfego de atualização automática, baixando dados de sites confiáveis, mas com volume alto para períodos não adequados do dia.

2.5. Problemas de segurança da informação

Bem como na questão de segurança da rede, a segurança de informação é afetada se não controlado os impactos que BYOD expõe: Imagine que os dados da organização podem sair da empresa e ficarem expostos. O

roubo de informações, pela falta de controle sobre os equipamentos pessoais aumenta o risco de vazamento de informações sensíveis.

Um dos maiores desafios é entender quem gerencia os equipamentos e tem o poder de administração destes. O dispositivo é do usuário, não da corporação. Entender e responder esta situação pode facilitar a definição das políticas de controle e domínio de rede da empresa.

Ponto importante para a política de BYOD é a separação do conteúdo corporativo e do conteúdo pessoal. O risco neste caso está para ambos os lados, empresa e usuário, pois um dispositivo pessoal pode conter informações que colocam o usuário a risco ou situações constragedoras, e podem, sem conhecimento, estar compartilhadas.

Cabe a empresa eleger um regulamento bem definido, deixando claro as regras e condições do uso. Esses regulamentos devem apontar no sentido de fazer recomendações técnicas e boas práticas de utilização, adotando cláusulas de confidencialidade da informação.

2.6. Redes de computadores

Segundo Tanenbaum (TANENBAUM, ANDREW S., 2003), uma rede de computadores é um conjunto de computadores e dispositivos interconectados por uma única tecnologia, que se comunicam.

Na prática, as redes de computadores, através de seus dispositivos ativos, *switches*, roteadores e pontos de acessos sem fio, integram computadores e dispositivos móveis. O objetivo é o compartilhamento de recursos e informações.

Estes ativos de redes são equipamentos que tem capacidade de operação e são bastante parecidos com computadores, contando com itens como memória e *chipset*, portanto, são limitados e geram atrasos de processamento aos pacotes.

Fazer um investimento em redes de computadores é, em geral, bastante difícil, pois envolve uma parcela grande do faturamento. A idéia é sempre absorver as novidades do mercado e principalmente trazidas pelos usuários, com a tecnologia atualmente instalada. Nos dias de hoje, o

investimento em equipamentos *wireless* deve ser visto com prioridade, frente a expansão de redes móveis sem fio.

Contudo, os equipamentos devem suportar práticas de segurança capazes de atender ao aumento de complexidade e riscos que surgem com as redes móveis. Praticamente todos os dispositivos móveis hoje são capazes de utilizar a comunicação sem fio, e muitas vezes, com mais de uma interface de conexão.

Figura 4 - Exemplo de dispositivos de uma rede

Fonte: Cuiket, 2013

De acordo com Jarrett Benavidez (COMPUTERWORLD, 2013), diretor da Trustwave para América Latina, a mobilidade deixou de ser uma opção para se tornar um dado da realidade. "Não há mais como negar totalmente o acesso às redes empresariais por *smartphones*, *tablets* e computadores pessoais portáteis".

Isto inclui também aumento nos níveis de vulnerabilidade e todos os tipos de ameaças que dispositivos móveis acrescentam aos sistemas, dados e aplicações. O aumento da violação de políticas de segurança e ao uso de aplicativos móveis inseguros, está criando riscos de segurança em níveis cada vez mais elevados.

2.7. Redes Wireless

A comunicação sem fio é, sem dúvida, a parte da rede que irá atender ao maior número de dispositivos. Redes sem fio são cruciais para o BYOD. De acordo como o site the Pulse, que revela uma pesquisa da Gartner, 80% dos clientes da Gartner terão de atualizar suas redes WiFi para suportar a demanda e requisitos do novo modelo (PULSE, 2013).

O custo desta atualização da rede sem fio pode ficar bastante alto, pois os equipamentos devem atender os requisitos mínimos para tecnologia. Além dos requisitos de funções, provavelmente o número de pontos de acesso sem fio irá aumentar, devido o crescimento de requisições e clientes conectados, pode ser necessário um balanceamento de carga em pontos de acesso.

Figura 5 - Exemplo de dispositivos de uma rede wireless

Fonte: Cuiket, 2013

Sem uma solução de rede completa, os gerentes não tem a visão dos dispositivos BYOD, e sem adequação aos equipamentos, não estão aptos para controlar os riscos que os dispositivos *wireless* pessoais podem trazer.

Vários fatores devem ser considerados para cobrir o impacto da mobilidade nas redes, conforme o número de usuários cresce. Devido a sensibilidade do *wireless*, que utiliza o padrão CSMA/CA para ordenação de pacotes, qualquer tipo de problema de latência é muito mais aparente, e o aumento de desempenho passa a ser essencial.

Aqui não cabe apenas aos dispositivos de uso como computadores, *smartphones* e *tablets*. O risco do BYOD também recai em um ponto de acesso wireless instalado inadvertidamente por um usuário, causando uma falha de segurança, muitas vezes de alto risco.

Um ponto de acesso sem fio instalado sem controle pode fazer com que o sinal *wireless* cubra áreas fora da empresa. Isto expõe a rede e cria diversos pontos de fragilidade e problemas de segurança para a empresa. É possível acessar a rede interna da empresa estando do lado de fora, a partir daí, soma-se riscos.

Outro ponto muito importante a ser levantado, é o acesso a dispositivos que geram sinais de rádio frequência em ambientes críticos, como fábricas ou hospitais. A inserção destes equipamentos, ou o aumento do índice de emissão, pode interferir em sistemas críticos.

2.7.1. CSMA/CA

Diferente de redes ethernet, redes wireless utilizam um protocolo de colisão *carrier sense multiple access with collision avoidance* (CSMA/CA), ou acesso múltiplo com verificação de portadora com prevenção de colisão.

O CSMA/CA é um método de transmissão que faz um controle de envio de pacotes, o que contribui para a redução de colisões em uma rede. Antes de transmitir um pacote, o dispositivo avisa sobre a transmissão e aloca um tempo de uso de canal. Deste modo, evita que dispositivos tentem transmitir sem antes escutar o meio e verificar a disponibilidade do canal.

Os dispositivos de uma rede *wireless* utilizam o CSMA/CA, escutando o meio para transmissão. Pode-se imaginar que com o aumento dos dispositivos dentro de uma mesma área, o desempenho seja reduzido, pois cada estação deve esperar até que o meio esteja livre para transmitir. Para evitar as colisões no ambiente sem fio é utilizado um recurso chamado *request to send* (RTS), solicitar para enviar e *clear to send* (CTS), livre para enviar. Conforme o modelo a seguir:

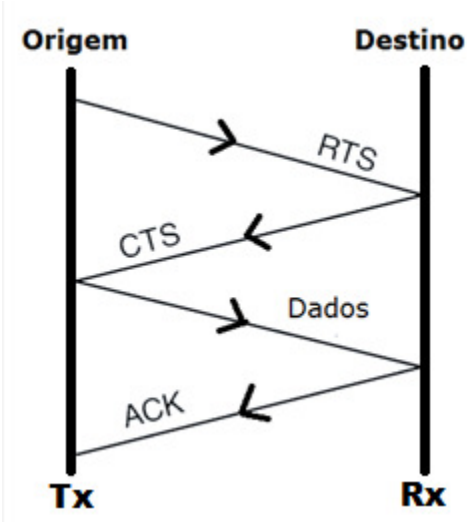

Figura 6 - Sinalização RTS, CTS

Fonte: DELTEC, 2013

2.8. Fundamentos de segurança

O conceito de BYOD, onde os usuários utilizam seus próprios equipamentos no ambiente de trabalho é um caminho sem volta. No entanto, é necessário que as empresas analisem os riscos a que estão expostas com a aceitação a este modelo.

Com o BYOD, sem a definição de políticas e regras adequadas, cresce a possibilidade de abertura de brechas para ataques à segurança e vazamentos de informações.

De acordo com a norma ABNT NBR ISO/IEC 27002:2005, “segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.”

Ainda de acordo com a mesma norma, “A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio”.

Entender e criar uma política de segurança de informação ajuda a nortear a gestão de segurança e a administração em BYOD. Os níveis de administração sobre os dispositivos e aplicações devem estar muito bem mapeados e o administrador deve, ao menos, estar ciente dos pontos de falha.

A NBR ISO/IEC 27002 define diretrizes gerais sobre práticas para a gestão da segurança da informação. Aconselha-se fortemente a leitura para amparo na criação de uma boa política e ferramentas de auditoria de segurança da informação.

Os dispositivos móveis possuem fragilidades que exige da TI uma política estruturada, tentando abranger todos os limites. Redes *wireless* permitem o acesso a recursos corporativos por meio de redes que estão longe da visão da corporação e das suas políticas de segurança.

Os principais pontos que orientam a implementação de uma política de segurança são confidencialidade, integridade e disponibilidade.

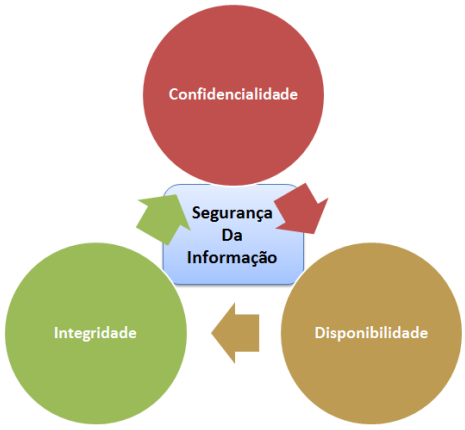

Figura 7 - Premissas de segurança da informação

Fonte: Autoria própria

- **Confidencialidade**: Limita o acesso à informação às entidades legítimas, ou seja, é a garantia de que a informação é acessível somente por pessoas autorizadas.
- **Integridade**: tende a garantir que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças, manutenção e descarte de informação;
- **Disponibilidade**: garante que a informação esteja sempre disponível para o uso legítimo, ou por usuários autorizados pelo proprietário da

informação. É a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos da organização sempre que necessário.

3. SOLUÇÕES TÉCNICAS PARA O GERENCIAMENTO DE BYOD

Este capítulo descreve algumas soluções e boas práticas para aqueles que entendem a importâncias da aceitação de BYOD para observar riscos e falhas, que torna um simples telefone móvel um dispositivo a ser gerenciado.

3.1. Mapear os objetivos da empresa

As regras da adoção de BYOD precisam ser simples para o setor de tecnologia da informação e para os usuários. A empresa deve definir o que poderá ou não ser acessado e como o acesso será feito: Dispositivos da corporação ou pessoais.

Para que a empresa possa definir a melhor solução para sua rede, os requisitos de segurança e necessidades devem estar devidamente mapeados, aliado a cota de investimentos disponível.

3.2. Cadastrar os equipamentos

Entender quem são os usuários e quais dispositivos serão utilizados garante mais confiança e segurança para a empresa e ajuda na classificação de equipamentos e políticas.

Mapeie os tipos de usuários, necessidade e tipo de acesso. Há diferentes tipos de usuários em qualquer companhia e compreendê-los é essencial para entender a real necessidade de cada um.

Classifique e conheça os dispositivos de usuário que mais irão viajar, que acessam informações crítricas e aplicativos utilizados nos dispositivos do usuário.

Conhecer os dispositivos assegura melhor controle de vírus e fragilidades, aumentando a garantia a qual a TI tem de se preparar.

3.3. Classificação das informações

Classificar a informação e como será acessada. Dependendo da criticidade da informação, pode-se optar por ser acessada somente por dispositivos puramente empresariais.

Criar políticas que definam e dividam a diferença e limite entre a informação pessoal e a informação corporativa. Preferencialmente a informação deve ser salva somente em um servidor, e para facilitar este trabalho, existem soluções em nuvem que gerenciam documentos.

3.4. Formalização dos processos

Regras claras dentro da empresa, definindo e expondo os métodos de acesso e os sistemas utilizados. Apresentar as aplicações necessárias e políticas de suporte. Deixar claro e fazer com que os funcionários conheçam os procedimentos relativos ao BYOD.

Expor o que pode e o que não pode com o intuito de traçar limites e mostrar os efeitos inerentes aos excessos. Muitas vezes o BYOD pode não ser utilizado na organização, ou em determinado setor. Exemplo disto, em um ambiente clínico ou fabril, onde pode existir regras que pribam o uso de equipamentos móveis, sob risco de interferência a equipamentos críticos.

Aproxime a TI aos recursos humanos da empresa e do gerente e crie uma estratégia para dispositivos perdidos, roubados e de funcionários que saem da empresa. Deve-se aplicar na política uma regra que obriga todos os dispositivos BYOD a passarem por um processo de limpeza, na saída de um funcionário.

3.5. Preparar a rede

Diante do fato que o BYOD está inserido no Brasil, não esperar a rede sofrer gargalos ou falhas é o cenário recomendável. É praticamente impossível prevenir que os colaboradores levem os seus equipamentos pessoais para

dentro de redes corporativas, escolares, etc. Com a mobilidade, são inúmeras as possibilidades de dispositivos com capacidade de acesso a *Internet*.

É claro que buscar a excelência para atender a demanda crescente com segurança e qualidade requer altos custos de infraestrutura. Por isto, a TI deve fazer um estudo amplo das necessidades e de onde se pretende chegar e o que deve ser realizado.

Para a utilização do BYOD é necessária uma solução que envolva desde a conectividade, até a existência de uma estrutura no servidor para suportar a demanda de recursos. “Muitas empresas hoje, por um excesso de zelo na segurança têm políticas muito restritivas, onde nada se pode fazer, e com isso, a empresa acaba perdendo em agilidade e produtividade que, por consequência, podem levar as empresas a se tornarem menos competitivas. Um primeiro movimento que as empresas precisam fazer é investir no próprio estudo do assunto, para ver de que forma empresas que já usam do recurso estão se beneficiando, afirma Rafael Araújo, Diretor Técnico da Teltec Solutions (TELTEC SOLUTIONS, 2013).

Para configuração de equipamentos, algumas funções são listadas abaixo como objeto de estudo e devem entrar como premissa para configuração de equipamentos e redes para alocação de BYOD:

- **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 dispositvivos 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 (INTEL, 2013).
- **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.

3.6. Wireless

O ambiente sem fio requer cuidados especiais. Com o aumento de dispositivos com interface sem fio, maior também a interferência sobre o meio. A interferência aumentará na medida que os dispositivos irão transferir dados.

O controle no ambiente *wireless* deve, por exemplo, ser aplicado para evitar interferência entre APs, evitando que equipamentos dentro da mesma rede concorram na mesma frequência. Os equipamentos que operam na faixa

de 2,4GHz são os mais comuns atualmente, sendo possível encontrar equipamentos operando na frequência de 2,4GHz e 5GHz para equipamentos *wireless*.

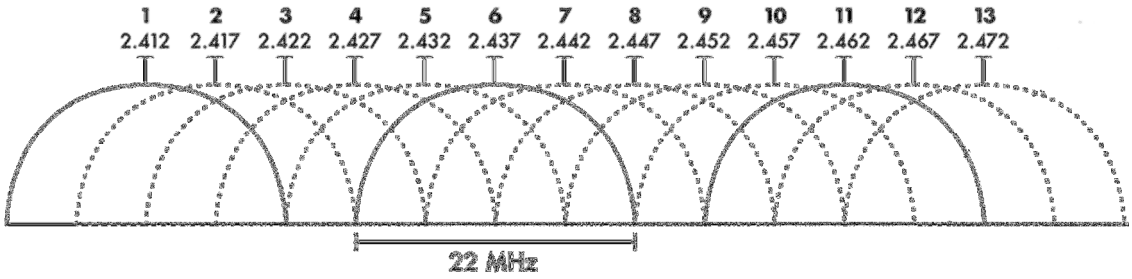

Figura 8 - Distribuição canais wireless em 2,4GHz no Brasil

No Brasil, a faixa de frequência disponível para equipamentos *wireless* é de 2,412GHz até 2,472GHz, ou dos canais 1 ao 13. Sendo que sugere-se o uso de canais distantes, para evitar interferências, como por exemplo os canais 1, 6 e 11.

O ambiente *wireless* requer monitoramento constante e permanente do ambiente, dispositivos e da rede corporativa da empresa. O monitoramente irá permitir que se possa traçar uma linha de uso e consumo de recursos e capacidade dos equipamentos.

Alguns equipamentos já fazem este controle automaticamente, tanto para alocar a melhor disposição de frequências para equipamentos conhecidos, alterando os APs em uma planta, como identifica um ambiente poluído e tenta alocar uma frequência em um canal mais livre de interferência.

Este controle vai depender muito do equipamento que se utiliza. Existem equipamentos que permitem detectar, além da melhor frequência, os tipos de pontos de acesso não autorizados incluindo *soft* APs e *hotspots* móveis que estão dentro da área de cobertura do equipamento principal no âmbito de segurança. Isto evita que intrusos e *rogue* APs, acessem a rede da empresa.

Focado em BYOD, existem equipamentos que permitem automaticamente localizar na rede da empresa, com precisão, qualquer dispositivo sem fio. Esta identificação automática pode ainda, conforme necessário ou políticas pré-determinadas, detectar e bloquear, em tempo real, dispositos móveis não autorizados.

3.7. MDM (Mobile Device Management)

Com o objetivo de controlar redes *wireless* corporativas, determinando quais usuários podem acessar qual tipo de conteúdo na rede, de acordo com perfis customizáveis de acesso.

As ferramentas de MDM ou gerenciamento do dispositivo móvel busca maneiras de proteger os ambientes corporativos de acessos indevidos, feitos por meio de dispositivos móveis.

Esse tipo de solução trabalha com filtros e registros dos acessos. Gerenciadores analisam e acusam a entrada de dispositivos dentro do ambiente corporativo. Esta ferramenta ajuda tanto na proteção de filtros, como são capazes de desligar o dispositivo ou até mesmo apagar todos os dados.

O XCube Labs, desenvolvedor de aplicações para dispositos móveis, mostra que a plataforma MDM atua basicamente em Segurança, Monitoramento e Configuração, criando um ambiente de monitoramento e provisionamento constante e bastante confiável, como mostrado na figura seguinte.

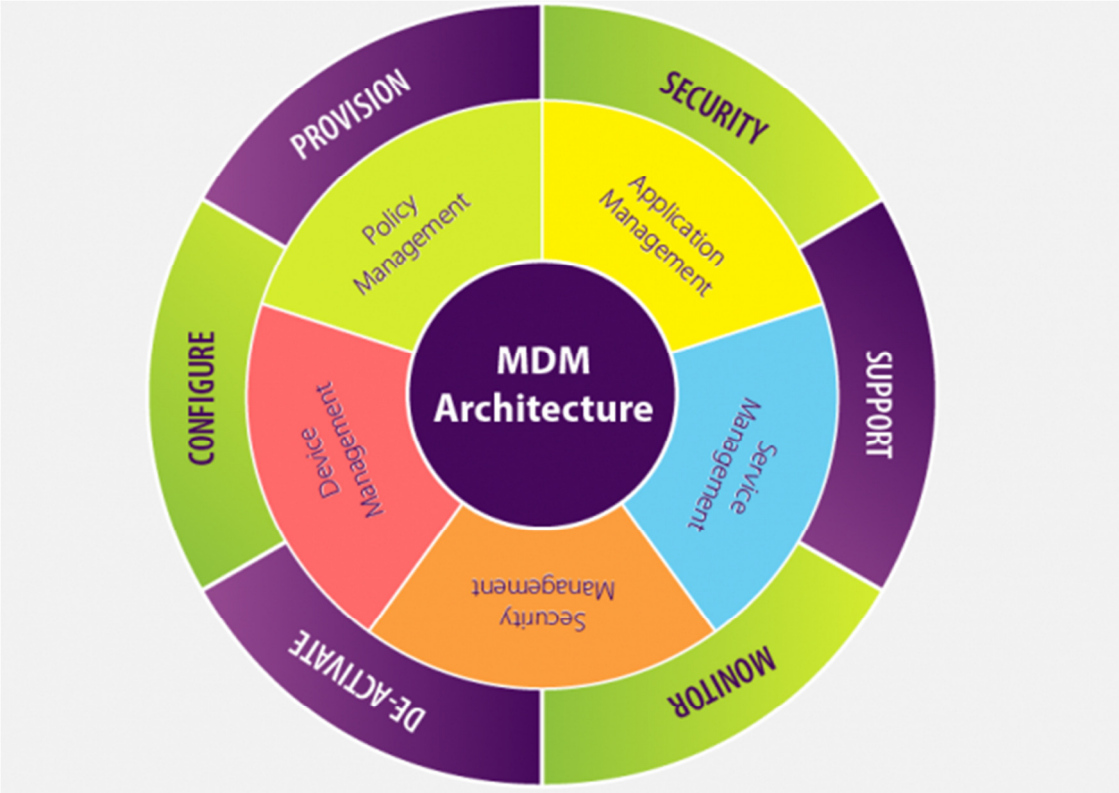

Figura 9 - Modelo de estrutura MDM

Fonte: [X]Cube Labs, 2013

Contudo, o fato do MDM atuar sobre a estrutura física do dispositivo, pode causar irritações de usuários como gerentes de TI. Para o dono do dispositivo, não é interessante, por exemplo, ter seu dispositivo formatado.

MDM por si só não gerencia o BYOD já que os dispositivos pessoais não possuem o agente do MDM de modo nativo. Cabe a TI, atráves da documentação do modelo de implantação de BYOD, incentivar os usuários a instalar o aplicativo.

Cabe associar a soluções MDM a uma estrutura de soluções de controle de rede, como o *Network Access Control* (NAC), podendo controlar o acesso tanto dos dispositivos conectados a rede sem fio corporativa ou de visitantes, como dispositivos intrusos a rede, como *rogue* Aps ou um equipamento com interface *wireless* integrado levado por um usuário, por exemplo. (ESECURITY PLANET, 2013).

3.8. Treinamento e conscientização constantes

Cabe tanto ao setor de TI como para os usuários o treinamento e apresentação do modelo de BYOD. Todos devem estar cientes da importância de apresentar previamente suas dúvidas e necessidades, bem como deve ser de conhecimento público documentos da política de BYOD.

4. CONSIDERAÇÕES FINAIS

Com o crescimento rápido na quantidade de dispositivos móveis, e o aumento de capacidade de processamento, a tendência é que estes dispositivos sejam levados expontaneamente para dentro das empresas. Este é o conceito de BYOD.

As empresas, por sua vez, recebem uma maior carga de tráfego dentro da rede, que pode afetar tanto o desempenho das redes, como a segurança dos dispositivos e aplicações.

É fundamental o planejamento e a definição dos níves de segurança e gerência que se deseja, evitando que o BYOD torne-se mais caro para a empresa em investimento de máquinas e aplicativos, do que a aquisição de dispositivos para funcionários.

As políticas de segurança devem ser levantadas e apresentadas de modo formal, deixando clara as condições para que os profissionais possam utilizar seus equipamentos móveis no ambiente corporativo sem comprometer a segurança da informação e sem interferir no rendimento profissional.

Quanto antes empresas e admisnitradores se prepararem, menor o impacto e maior o sucesso.

BYOD não é tecnologia, é um conceito para a prática da entrada de dispositivos externos a rede. Contudo, esta prática exige intervenção direta na rede, e não adianta remar contra a maré. O desafio é aliar e prover comodidade e produtividade aos funcionários. Esta combinação tem tudo para dar certo.

5. REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS E TÉCNICAS - ABNT. **NBR ISO/IEC 27002:2005 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da Informação**. Rio de Janeiro: ABNT, 2005.

BRADLEY, Joseph; LOUCKS, Jeff; MACAULAY, James. **BYOD: uma perspectiva global.** Cisco IBSG Research & Economics Practice, 2012.

COMPUTERWORLD. **BYOD não é mais tendência no Brasil, diz Gartner.** 2013. Disponível em < http://computerworld.uol.com.br/negocios/2013/04/09/byod-nao-e-mais-tendencia-no-brasil-diz-gartner/> Acesso em 17/08/13, 10:48.

COMPUTERWORLD. **Empresa reforça proteção de rede para reduzir riscos do BYOD.** 2013. Disponível em < http://computerworld.uol.com.br/seguranca/2013/06/03/empresa-reforca-protecao-de-rede-para-reduzir-riscos-do-byod/> Acesso em 17/08/13, 11:14

COPELAND, Rebecca; CRESPI, Noel. **Analyzing Consumerization - Should Enterprise Business Context Determine Session Policy?.** IEEE, 2012

CUIKET. **Fotos empresas: Galeria de fotos de produtos, serviços e trabalhos das empresas brasileiras**. Disponível em <http://www.galeria.cuiket.com.br> Acesso em 26/08/2013

DELTEC. **Acesso aos Meios em WLANs: CSMA/CA – CCNA**. 2013. Disponível em <http://www.dltec.com.br/blog/cisco/acesso-aos-meios-em-wlans-csmaca-ccna/> Acesso em 24/08/2013, 18:01

ESECURITY PLANET. **BYOD Fuels NAC Comeback**. Disponível em <http://www.esecurityplanet.com/network-security/byod-fuels-nac-comeback.html> Acesso em 25/08/2013, 19:33

INTEL. **Rede sem fio**. 2013. Disponível em < http://www.intel.com/support/pt/wireless/wlan/sb/cs-025323.htm> Acesso em 25/08/2013, 18:54

MANAGEMENT, INFORMATION. **Solução acelera resolução de problemas em redes BYOD e VoIP.** 2013. Disponível em < http://docmanagement.com.br/07/04/2013/solucao-acelera-resolucao-de-problemas-em-redes-byod-e-voip/?doing_wp_cron=1376529461.8781640529632568359375> Acesso em 17/08/13, 12:00.

PULSE, THE. **Plan Now for the Hyperconverged Network.** 2013. Disponível em < http://blog.xo.com/networking/plan-now-for-the-hyperconverged-network/> Acesso em 20/08/13, 22:12

SOLUTIONS, TELTEC. **BYOD e consumerização: o que são e como utilizar.** 2013. Disponível em < http://blog.teltecnetworks.com.br/category/byod/> Acesso em 21/08/13, 22:08

TANENBAUM, Andrew S. **Redes de Computadores.** 4ª ed., Rio de Janeiro: Editora Campus, 2003

[X]CUBE LABS. Mobile Device Management enable manage and secure your mobile environment. Disponível em <http://www.xcubelabs.com/blog/mobile-device-management-enable-manage-and-secure-your-mobile-environment/> Acesso em 25/08/2013, 19:19