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

BRUNO GARANHANI

BYOD – BRING YOUR OWN DEVICE

MONOGRAFIA

CURITIBA
2013

BRUNO GARANHANI

BYOD – BRING YOUR OWN DEVICE

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. Kleber Kendy Horikawa Nabas

CURITIBA
2013

RESUMO

A presente monografia apresenta uma abordagem sobre o fenômeno global que está tomando conta de grandes corporações chegando às médias e pequenas empresas. Atualmente, a tecnologia está evoluindo em um nível muito acelerado de modo que os próprios consumidores levam seus dispositivos a qualquer lugar, desejam estar conectados a todo o tempo. O novo conceito chamado BYOD (*Bring Your Own Device*) tem como principal característica a mobilidade, fazer com que as pessoas além de trabalharem com seus próprios dispositivos, tenham rapidez e produtividade em suas tarefas. O projeto contextualiza como este movimento beneficia diferentes áreas de uma empresa começando por um planejamento, análise de custos, riscos envolvidos, políticas de segurança bem definidas até as responsabilidades por parte da empresa e funcionários. Ao final deste trabalho serão demonstrados o escopo de um estudo de caso de implementação do conceito.

Palavras-chave: Mobilidade. Consumerização. NAC. BYOD. Wireless.

ABSTRACT

This monograph presents an approach about the phenomenon that is taking over large corporations coming to the medium and small enterprises. Nowadays, technology is evolving at a very fast so that consumers bring their own devices anywhere, want to be connected all the time. The new concept called BYOD (Bring Your Own Device) has as main characteristic mobility, make people besides working with their own devices, have speed and productivity tasks. The project contextualizes how this move benefits from different areas of starting a business by planning, cost analysis, risks, security policies and set up the responsibilities for the company and employees. At the end of this work will be demonstrated the scope of a case study of the implementation of the concept.

Keywords: Mobility. Consumerization. NAC. BYOD. Wireless.

LISTA DE SIGLAS

AD – Active Directory

IAM – Identity and Access Management

IP – Internet Protocol

TI – Tecnologia da Informação

BYOD – Bring Your Own Device

NAC – Network Access Control

DAAAR – Detecção, Autenticação, Avaliação, Autorização, Redemediação

PCI DSS – Payment Card Industry Data Security Standard

SSID – Service Set IDentifier

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

O capítulo introdutório a seguir abordará sobre o tema proposto – *BYOD* (*Bring Your Own Device*) no qual serão apresentados utilização do conceito e seus respectivos aspectos.

1.1 TEMA

Com o passar dos anos muitos consumidores, exclusivamente boa porcentagem classificados como funcionários estão adquirindo novos dispositivos portáteis, como tablets, smartphones que através de aplicativos controlam e administram melhor suas atividades. Cada vez mais estes dispositivos apresentam interfaces avançadas e de forma acessível para o usuário, por isso torna o consumo em uma escala crescente e de grandes perspectivas para o futuro. A utilização destes dispositivos vem sendo aceita com “bons olhos” no meio corporativo, pois o funcionário tem a flexibilidade para desenvolver suas atividades tanto no ambiente de trabalho como em casa.

Segundo a pesquisa da Cisco IBSG realizada no segundo trimestre de 2012 na qual foram entrevistados 600 gestores em TI locados em empresas dos EUA, “noventa e cinco por centro dos tomadores de decisão em TI disseram que suas empresas apoiam o BYOD de alguma forma. Igualmente importante foi a atitude deles em relação ao BYOD. Sem minimizar os desafios impostos pelo BYOD, 76 por cento o consideraram “bastante” ou “extremamente” positivo para os departamentos de TI” (CISCO IBSG,2012).

A consumerização está mudando o cenário de investimentos no mercado de TI, pois as empresas pretendem mais investir em soluções de segurança do que atualizar suas estações de trabalho por exemplo. O consumidor final incentiva este tipo de expansão e se adapta a estas mudanças rapidamente, então o ambiente se torna propício para a utilização destes dispositivos. Fatores prós e contras serão debatidos ao longo do trabalho, mas o ponto de maior equilíbrio é como estabelecer políticas de segurança confiáveis em um mundo sem fronteiras? Contudo, há grandes desafios consequentes nos controles de acesso aos sistemas e as informações confidenciais da organização.

Pensando nestes efeitos, percebe-se a necessidade real da elaboração de Políticas de Segurança para aplicação do BYOD com o objetivo de

aproveitar os recursos ao máximo minimizando riscos à organização e privacidade do usuário.

1.2 OBJETIVOS

Nesta sessão serão trabalhados objetivo geral e objetivos específicos.

1.2.1 OBJETIVO GERAL

O objetivo do presente trabalho é abordar a utilização do conceito BYOD em redes corporativas destacando o uso de políticas de segurança adequadas para dispositivos de acesso.

1.2.2 OBJETIVOS ESPECÍFICOS

- Identificar as boas práticas para implementação da tecnologia através das políticas de segurança;
- Observar prós e contras para aplicação do BYOD em redes corporativas;
- Demonstrar escopo de estudo de caso aplicando o conceito.

1.3 JUSTIFICATIVA

Através da alta evolução tecnológica nos últimos anos somada ao fator “consumerização” tornou-se “necessidade” o gerenciamento ativo de redes corporativas pelos departamentos de segurança da informação. Elementos como produtividade e crescimento organizacional são consequências de uma estratégia BYOD bem implantada o que também contribui para redução de custos e otimização de equipamentos destinados aos usuários. Pretende-se demonstrar de que forma a tecnologia de segurança da informação vem sendo aplicada adequadamente, com propósito de preservar a integridade do negócio e prevenção contra riscos.

1.4 PROCEDIMENTOS METODOLÓGICOS

O material retirado para desenvolvimento do trabalho por se tratar de um assunto recente, maior parte foi retirado da Internet, entre artigos científicos, opiniões de gestores de TI, revistas e pesquisas realizadas em grandes empresas. O Estudo de Caso foi desenvolvido com base em implantações de projetos realizadas pelo aluno onde retirou parte das ideias para apresentação do tema. O processo como um todo contribuiu para o aprendizado do BYOD e aperfeiçoamento das ferramentas utilizadas.

1.5 EMBASAMENTO TEÓRICO

A utilização de dispositivos móveis como tablets e smartphones tornou-se frequente dentro de ambientes de trabalho, para as áreas de TI uma questão de controle e visibilidade. O fator da “consumerização” ajuda a desenvolver dispositivos com plataformas de aplicativos mais inteligentes e serviços personalizados, fatores como “*clouding*” e “redes sociais” são alguns dos recursos conhecidos dos *mobiles*. Conforme explica Oltsik (2012), os resultados desta mobilização forçam as organizações de TI a estabelecerem algum nível de segurança na rede, devido ao rápido crescimento da utilização de dispositivos sem fio no local de trabalho, também destaca a criação de regras para classificação dos níveis de segurança. O fluxo destas informações deve ser administrado de forma segura afim de que as equipes de segurança mantenham as funções abordadas no *NAC (Network Access Control) - Detection, Authentication, Assessment, Authorization e Remediation*.

Segundo Stallings (2005) no contexto de segurança de rede, o controle de acesso permite controlar e limitar o acesso a sistemas e aplicações por meio de enlaces de comunicação. Para um controle consistente toda entidade deve ser identificada antes do acesso, assim as condições estabelecidas (direitos de acesso) serão determinados de acordo com o perfil de acesso do usuário.

Em um ambiente BYOD o ponto de maior impacto está voltado ao usuário final, na medida em que os dispositivos são conectados a rede a vulnerabilidade aumenta, problema de diversidade de equipamentos, sistemas operacionais e protocolos de rede não suportados são alguns exemplos. A

capacidade de identificar rapidamente um problema com o usuário final e isolá-lo torna-se um requisito essencial para reduzir a complexidade do ambiente, diagnosticar e corrigir o problema em tempo hábil é reflexão de um sistema bem planejado.

Pesquisas recentes referentes ao tema apontam resultados estimulantes para utilização de dispositivos móveis nas empresas, o potencial transformador do BYOD proporciona ao funcionário decidir como, quando e com quais ferramentas o trabalho é realizado. Uma pesquisa realizada pela Cisco IBSG (2012) relata que a necessidade ou desejo dos funcionários de serem móveis e se conectarem à rede da empresa remotamente está impulsionando o crescimento de smartphones, tablets e outros dispositivos móveis. A pesquisa destaca também que os principais benefícios do BYOD são produtividade, satisfação no trabalho e custos de hardware reduzidos para a empresa.

Normas elaboradas pela PCI Security Standards Council (2010) como a *PCI DSS 9.1* - define o isolamento de equipamento utilizando segurança física e *10.2.5* - mecanismos de autenticação e identificação do usuário, ajudam a tornar o ambiente menos propício a ataques. Podemos citar também o padrão de autenticação 802.1x, método de bloqueio das portas sem o uso de forma física, permitindo acesso somente aos equipamentos e usuários devidamente identificados.

1.6 ESTRUTURA

A monografia é constituída por 4 capítulos. O capítulo 1 tratará da parte introdutória, aborda sobre o tema, objetivos a atingir, a justificativa sobre o estudo desenvolvido. Outros tópicos como embasamento teórico, procedimento metodológico e a estrutura da monografia também são discutidos nesta primeira parte.

Em relação ao capítulo 2 trata do referencial teórico do projeto. Questões relacionadas à expansão do BYOD, o crescimento móvel, implantação de políticas de segurança, além de mecanismos de defesa com objetivo de minimizar o risco de invasões são destacados. Alguns padrões de implantação são apresentados, bem como riscos e benefícios identificados após aplicação do conceito. Trata também da necessidade de um planejamento estratégico detalhado a fim de garantir a segurança adequada a todas as áreas envolvidas.

Já o capítulo 3, apresenta o escopo do estudo de caso a ser implantando em cliente, associa-se a parte conceitual da criação de políticas de

segurança e hierarquia dos controles de acesso (modelo RBAC) a prática da aplicação de perfis conforme definidos pelos departamentos de segurança da informação. Estes perfis podem estar associados ao tipo de dispositivo, tipo de acesso, localização do usuário, credenciais fornecidas, etc. Espera-se com a implantação do BYOD proporcionar meios para o gerenciamento seguro da rede como foco principal os dispositivos móveis, obter maior visibilidade do ambiente como um todo.

No capítulo 4, são apontadas as conclusões finais sobre todo o estudo realizado do BYOD, em seguida as referências utilizadas para desenvolvimento da monografia.

2 REFERENCIAIS TEÓRICOS

2.1 CRESCIMENTO MÓVEL

O BYOD está impulsionando o crescimento móvel, isso se deve ao fator “mobilidade”, porque mesmo o profissional estando fora do seu local de trabalho ele consegue desenvolver as atividades como se estivesse dentro da empresa. De acordo com a pesquisa da Cisco IBSG, “quarenta e sete por cento dos funcionários nas empresas que entrevistamos são oficialmente designados “profissionais móveis”. Mas 60 por cento dos funcionários usam um dispositivo móvel no trabalho, 13 por cento a mais que os considerados oficialmente “profissionais móveis”, segue abaixo uma comparação entre os perfis de profissionais (CISCO IBSG,2012).

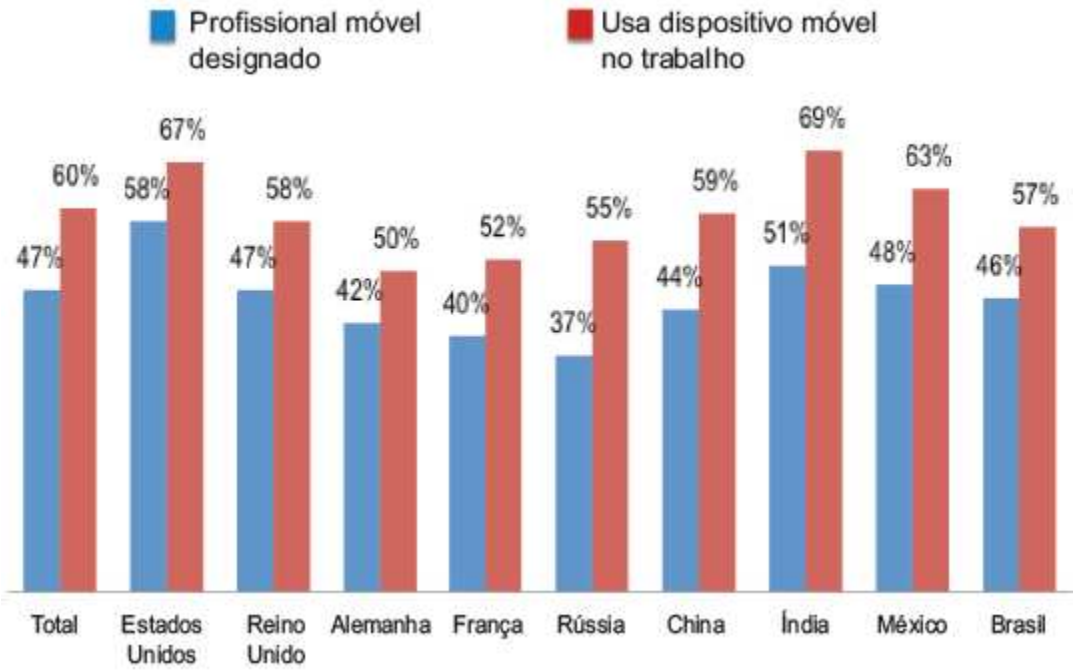

Figura 1. Perfil móvel designado x Perfil móvel no trabalho
Fonte: Cisco IBSG - Byod: uma perspectiva global, 2012.

O aumento desses dispositivos móveis em empresas é um fato real, as empresas devem mudar a maneira de gerenciar os dispositivos. Este progresso na mobilidade pode afetar a segurança dos dados da organização, controle de acesso, manutenção de plataforma, suporte a aplicativos e muito mais.

2.2 POLITICAS DE SEGURANÇA DA INFORMAÇÃO

As políticas de segurança devem ser estabelecidas a fim de garantir um nível de segurança adequado no ambiente corporativo. No item subsequente será abordado sobre alguns pontos relevantes.

2.2.3 IMPLEMENTAÇÃO DE POLÍTICA BYOD

Com o chamado fato da “consumerização”, aumenta a análise da implementação de uma política de BYOD em ambientes corporativos, principalmente em instituições de ensino onde normalmente é caracterizada por um ambiente de difícil controle e sujeita a qualquer tipo de ataque.

O primeiro passo seria o estabelecimento de regras, afirma Pinheiro:

> Devemos definir de quem é a propriedade do equipamento, quais os requisitos de segurança que o mesmo deverá cumprir, bem como quais as obrigações e limites de uso do mesmo. Há uma grande diferença em termos de gestão da TI, quando a empresa deixa de ser quem fornece o recurso e passa a ser beneficiária do uso do recurso particular de seu colaborador ou de um terceiro (PINHEIRO, 2012).

Alguns pontos importantes a serem estudados para criação das políticas de segurança para o BYOD conforme menciona Computer World:

- Definir o “uso empresarial aceitável” do dispositivo, como quais atividades são determinantes para beneficiar a empresa direta ou indiretamente;
- Definir o “uso pessoal aceitável” durante o horário na empresa;
- Definir quais aplicações permitidas e quais não o são;
- Listar os equipamentos que o departamento de TI vai permitir acesso às suas redes.

Em contrapartida temos outros itens a considerar como, por exemplo, políticas adicionais para os empregados, onde o funcionário mantém a confidencialidade das informações assegura a não concorrência, monitoramento para onde vão os dados e o mínimo de acesso aos dispositivos locais (servidores locais ou de aplicações importantes em produção). Por fim recomenda-se a limpeza regular e mais cautela na contratação do profissional na empresa (COMPUTER WORLD, 2013).

2.3 BYOD

Conforme Silveira “Trata-se de um fenômeno global onde envolve serviços, políticas e tecnologias que proporciona aos funcionários desempenhar atividades profissionais utilizando seus próprios equipamentos, como smartphones, tablets ou notebooks”, tal qual em um contexto mundial vem ganhando força entre as organizações potencializando aumento de produtividade e redução nos investimentos em dispositivos para o usuário. (SILVEIRA, 2013)

Nos tópicos a seguir iremos abordar sobre algumas condições que o mercado dispõe para utilização desta tecnologia.

2.3.1 BENEFÍCIOS E RISCOS DO BYOD

Os benefícios ofertados pelo BYOD são inúmeros, um exemplo é que ao longo do tempo os profissionais estão produzindo mais e aderindo com facilidade aos dispositivos móveis, como demonstra a pesquisa realizada pela Intel Corporation em 2012 com gestores de TI em alguns países (Estados Unidos, Alemanha, Austrália e Coréia do Sul), onde questionados se acreditam que um programa de BYOD traria benefícios de produtividade empresarial (Figura 2).

Figura 2. Pesquisa sobre benefícios esperados do Programa BYOD
Fonte: Intel Corporation – Insights on the Current State of Byod, 2012

Também foi levantado na mesma pesquisa os benefícios mais esperados na implementação do programa, onde determinados benefícios

contribuem diretamente no recrutamento de novos funcionários, pois reduz o tempo de treinamento e ciclos de substituição de computadores novos (INTEL, 2012).

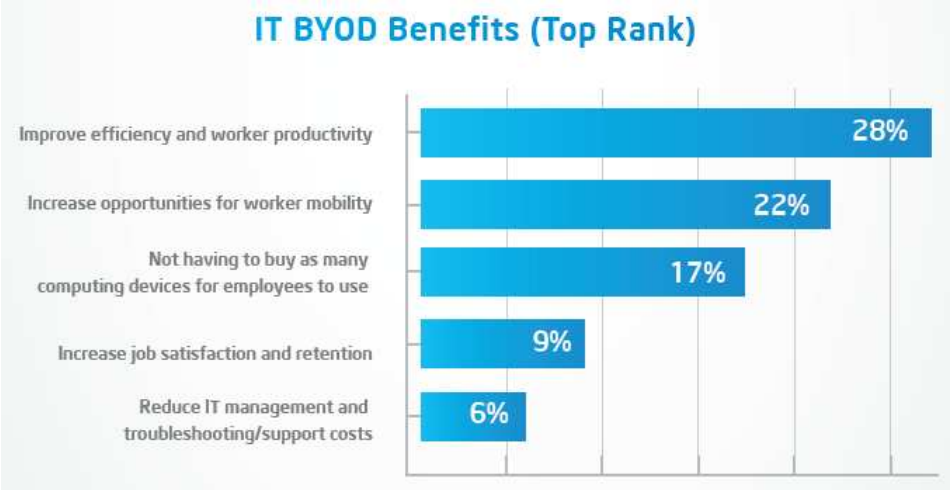

Figura 3. Pesquisa sobre os principais benefícios do BYOD
Fonte: Intel Corporation – *Insights on the Current State of Byod*, 2012

Segundo a Olhar Digital os benefícios que o BYOD traz para a empresa são significativos principalmente relacionados ao aspecto financeiro, se cada funcionário utiliza seu dispositivo pessoal para o trabalho diminui os custos de manutenção do parque de máquinas e possibilita a mobilidade em qualquer lugar da empresa, fica apenas o custo de manutenção das contas dos funcionários. O empregado também é beneficiado, pois além de desempenhar suas atividades com facilidade e rapidez, aumenta a produtividade contribuindo para o crescimento da organização (OLHAR DIGITAL, 2012).

Em contrapartida conforme relata pesquisa da Cisco IBSG, quando os funcionários utilizam seus próprios aplicativos, isso acarreta em possíveis custos para a empresa. Um exemplo prático é o aumento da largura de banda onde determinados aplicativos consomem mais do que o necessário por estarem combinados a uma serie de serviços (gráficos avançados, redes sociais, serviços de transmissão de mídias). Outro exemplo é o uso de ferramentas de colaboração não aprovadas, principalmente se estas ferramentas forem limitadas ou inadequadas, podendo implicar em plataformas descentralizadas e divergências de dispositivos sem padrão nenhum de acesso. Estas combinações devem ser planejadas e gerenciadas pelo departamento de TI, afim de não criar “gargalos” na rede ou futuros problemas para a empresa. (CISCO IBSG, 2012).

De um modo geral há forte aceitação do BYOD por parte dos líderes de TI da empresa, relata a pesquisa realizada pela CISCO IBSG, “quase 90 por cento aceita o BYOD de alguma forma, o que varia de apenas permitir dispositivos de propriedade dos funcionários na rede da empresa a oferecer suporte completo de TI para todos esses dispositivos...”, Estados Unidos e Índia destacam-se por oferecer suporte mais adequado para dispositivos de propriedade dos funcionários chegando a 30 por cento de suporte a todos os dispositivos. A nível Brasil as políticas implementadas ainda são generosas, a empresa em muitos casos compra os dispositivos e oferece aos funcionários ou permite que o próprio funcionário traga o seu dispositivo não levando muito em consideração as questões de aplicação das políticas de segurança.

2.3.2 ESTRATÉGIA PARA IMPLANTAÇÃO

O estudo para implantação do BYOD deve ser realizado de forma rigorosa, seguindo critérios definidos pelos departamentos de segurança da informação em conjunto com o estudo específico de aplicações de comunicação corporativa, conforme explica Silveira (2013), recomenda-se uma abordagem que cubra os seguintes tópicos:

- Avaliação das áreas com maiores necessidades de comunicação, considerando tanto a importância da comunicação quanto o volume de gastos telefônicos;

- Definição de usuários chave, como, por exemplo, colaboradores seniores ou gerentes capazes de gerar avaliações consistentes sobre a solução e contribuir na disseminação nas etapas seguintes;

- Determinação do período de testes, tempo em que o BYOD não será a única solução, mas uma alternativa. Este período deve ser suficiente para os usuários formarem impressões e avaliar a confiabilidade da solução;

- Estabelecimento de termos de compromisso com os usuários, contemplando, por exemplo, os dias e horários que ele está autorizado a utiliza o próprio dispositivo em atividades profissionais. Deve ser criadas regras que evitem o

uso do sistema em horários inadequados. Esta ação irá ajudar a amenizar o risco de problemas trabalhistas;

- Definição e avaliação dos aspectos de segurança, como por exemplo, que tipo de portas devem ser abertas e que tipo de permissões de rede devem ser dadas aos usuários. As informações levantadas devem ser confrontadas com as políticas de segurança da empresa.

Contudo, um planejamento estratégico auxilia na implantação do BYOD, mas ainda não existem padrões para implantação visto que o conceito ainda é recente e dispõe de estudos sobre a aplicabilidade.

2.3.3 DESAFIOS

Quando nos deparamos a uma tecnologia nova no mercado uma das primeiras reações que nos vem à tona é, quais os desafios da nova tecnologia? Na teoria totalmente viável na prática começam a aparecer os problemas. Entre alguns pontos mencionados por Nascimento podemos destacar “segurança da informação, pois dados intelectuais corporativos mantidos em um dispositivo pessoal precisam estar protegidos. O acesso a redes privadas necessitam ser controlados para evitar que programas maliciosos se propaguem caso o dispositivo esteja contaminado” (NASCIMENTO,2013).

A tendência leva o BYOD a crescer exponencialmente no mundo todo. Tratando-se de um novo conceito surgem novas ferramentas e plataformas desenvolvidas pelos fabricantes, mas traz consigo alguns desafios. Alguns pontos são importantes para discussão:

- Novos dispositivos: quais os níveis de acesso? Separar a rede corporativa dos visitantes (criar regras para separação);

- Identificação de equipamentos móveis: particular ou corporativo e localidade? Gerenciar os equipamentos internos, saber o que, quem e local onde está conectado a rede;

- Melhores práticas de rede e segurança: Padrões e normas para garantir o ambiente seguro devem ser adotados bem como monitoramento constante dos ativos de rede.

- Escalabilidade: Quanto mais equipamentos conectados, maior a complexidade da rede. *Throughput* de *switches* e *firewall* aumentam gradativamente sujeitos a futuros problemas.

- Mudanças dinâmicas: Gerenciar o crescimento e as mudanças no ambiente de forma granular a fim de evitar constantes transtornos com colaboradores e prejuízos para a organização.

2.3.4 SUPORTE TÉCNICO

Com a diversificação de modelos de equipamentos móveis disponíveis no mercado torna-se necessária o desenvolvimento da equipe técnica de TI para suporte a estes dispositivos. Há casos de departamentos de desenvolvimento interno da plataforma que adéquam os aplicativos para os dispositivos, tal modo que aumenta drasticamente os custos de manutenção. A Análise destes custos é indispensável no plano estratégico da implantação, pois requer esforço de horas de suporte previstas em caso de serviços externos.

Kaneshige (2012) destaca que o BYOD não só requer suporte de multiplataforma, mas também suporte multidepartamento. A empresa investe em alguma área de comunicação interna para tratar questões referentes ao BYOD. A divulgação de informações preventivas direciona o colaborador na agilidade do suporte e o auxilia nas questões de engenharia social.

Na maioria das organizações costuma-se estabelecer um padrão de quais dispositivos terão acesso à rede, a pesquisa da Cisco IBSG (2012) aponta “o Brasil como o ambiente de maior suporte para BYOD de todos os entrevistados, com 82 por cento das empresas com suporte a alguns outros dispositivos, comparado a 81 por cento nos Estados Unidos, 79 por cento no México e 71 por cento de média global”. Contudo, há diferentes níveis de suporte e entusiasmo. “Os Estados Unidos, Àsia e América Latina estão otimistas em relação às perspectivas do BYOD e desejam fornecer mais controle aos funcionários”. Contudo, este controle permite o desenvolvimento

da inovação, os profissionais encontram novas maneiras de realizar suas atividades e seus trabalhos tornam mais valorizados.

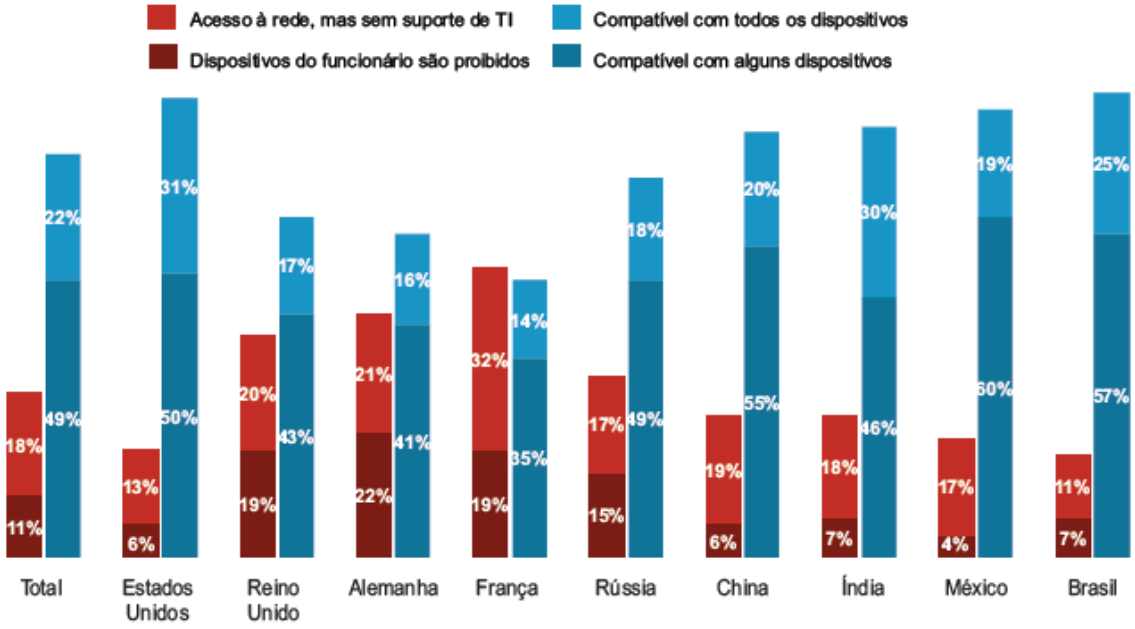

Figura 4. Pesquisa - Nível de suporte dispositivos dos funcionários
Fonte: Cisco IBSG - *Byod*: uma perspectiva global, 2012.

Também conforme mesma pesquisa, com o aumento dos níveis de suporte, os líderes de TI esperam que a quota de gastos de TI em dispositivos móveis cresça de 18 por cento em 2012 para 23 por cento em 2014. Outro dado importante é que 71 por cento das empresas fornecem suporte de TI para determinados dispositivos ou para todos os dispositivos de propriedade dos funcionários. Isso leva a crer que o BYOD exige das empresas maturidade de seus profissionais, qualificação técnica e bom entendimento nas funcionalidades do dispositivo.

2.3.5 PESPECTIVA

Segundo Mello, observa-se uma grande mudança de paradigmas na maneira com que a TI encara a manutenção da segurança em seu ambiente e também controle sobre os dispositivos de acesso, lembra também que nos últimos 10 anos uma gama de equipamentos cada vez mais portáteis e funcionais foram tomando espaço nas organizações, afirma que com o surgimento de aparelhos como *Black Berry* e do *IPhone*, estes aparelhos deixaram de ser apenas para ligações e tornaram-se definitivamente ferramentas de trabalho.

Não podemos levar em consideração apenas o perfil “híbrido” dos dispositivos móveis que torna a implementação mais complexa, mas devemos observar se essa variedade de tecnologia e protocolos é absorvida pelas soluções de gerenciamento e segurança na qual farão o controle destes dispositivos.

> Isto é um fato, não uma tendência – um fato que tem causado grandes preocupações as equipes de TI. Os gestores desta área precisam atuar sobre um dispositivo que traz, simultaneamente, dado e aplicações da vida íntima do usuário e das principais soluções de negócios da empresa (MELLO, 2013).

Esta tendência, se é que podemos chamar, é consequência do estouro na venda de equipamentos portáteis, pois o usuário tem interesse em conhecer o que há de novo e aberto a este tipo de mercado, consequentemente obtendo poder no processamento das informações e facilidade na hora de utilizá-las. É comum encontrarmos em reuniões dispositivos móveis no qual muitas vezes não pertence à organização, esta situação é cada vez mais frequente no meio corporativo. Os profissionais encaram seus dispositivos como ferramentas determinantes para concluir suas tarefas diárias e por isso buscam recursos de grande potencial.

É importante ressaltar a questão dos investimentos necessários de responsabilidade da organização, segundo Silveira:

> Em especial no que diz respeito à infraestrutura e às políticas necessárias a uma operação BYOD confiável, evitando efeitos colaterais tanto para o usuário quanto para as organizações, principalmente no que tange à segurança da informação e às questões trabalhistas (SILVEIRA, 2013).

No Brasil, a tendência é que as companhias apliquem este modelo de trabalho, afirma Ghassan da Olhar Digital “O BYOD tem sido aceito aqui no País pela alta gerência de grandes corporações e, através deles, nós funcionários conseguimos nos adequar a esta ferramenta. No entanto, o mercado brasileiro ainda carece de infraestrutura adequada e a solução está na mobilidade – em especial na cobertura Wi-fi” (OLHAR DIGITAL, 2012).

O ambiente de trabalho está passando por um momento de transformação, deixou de ser apenas um ambiente físico, mas uma mistura de ambientes físicos e virtuais, onde os funcionários estão trazendo suas preferências para trabalhar e o BYOD é o novo conceito em que a “colaboração” deve acontecer além das fronteiras da empresa, “*any-to-any”* conectados a todo o momento. Outras soluções no meio corporativo contribuem para que

esta tecnologia avance com maior rapidez como computação em nuvem, virtualização e repositórios de vídeos. Com base neste cenário as empresas estão procurando menos dispositivos fornecedores de tecnologia e mais ofertas de software que permitem alavancar os dispositivos portáteis (laptops, smartphones e tablets) que são utilizados no local de trabalho pelos funcionários. Os fornecedores de TI perceberam essas mudanças e começaram a desenvolver soluções de software adequadas para gerenciamento destes dispositivos móveis a fim de proteger a rede corporativa e os dados que por nela trafegam (CISCO SYSTEM, 2012).

2.4 MODELO DE CONTROLE DE ACESSO RBAC

O RBAC (*Role Based Access Control*) ou controle de acesso baseado em perfis é um modelo de controle de acesso para proteção de informações e recursos em ambientes informatizados. O RBAC é um método de acesso não direcionado, ou seja, os usuários têm de se submeter às políticas de segurança estabelecidas na organização.

Conforme Ferraiolo e Cugini (2006) a função do modelo RBAC é determinar as operações que determinados grupos ou usuários representam baseado no controle de acesso dentro da organização. As operações que estão associadas às funções determinam o conjunto de ações de permissão do usuário. O nível de abstração que os administradores de segurança da informação têm com a implementação do RBAC são extremamente vantajosas, pois centraliza os domínios de proteção local e facilita na aplicação das políticas de segurança.

Uma das formas de eficiência do método RBAC reflete a granularidade do modelo. Por um lado, quanto maior a granularidade no controle de acesso mais direitos de acesso cada atributo consegue obter para um usuário ou objeto da rede. Em contraste, quanto menor a granularidade mais baixa os direitos são concedidos a um grupo de usuários ou determinado objeto. Em resumo, o nível de granularidade é diretamente proporcional aos direitos dos grupos de acesso de objetos e/ou indivíduos.

2.5 NAC (Network Access Control)

Ao decorrer das últimas décadas, a preocupação tanto das empresas quanto administradores de rede eram de possuir fortes parceiros de negócios e aumentar o quadro de colaboradores, contudo esta concepção mudou com o avanço das redes e tecnologia. Agora, o foco é controlar o acesso aos dispositivos conectados à rede, visando bloquear conteúdos que não são de interesse da empresa. É por esse motivo que o NAC (*Network Access Control*) se tornou um mecanismo fundamental a segurança da informação a fim de evitar espiões e ataques à rede de negócios com uma completa estrutura de permissões e autorizações em diferentes níveis de acesso por diferentes grupos de usuários. “A tecnologia vem ajudando as empresas a aperfeiçoarem seus ambientes com novas metodologias das políticas de segurança, neste contexto o NAC auxilia as empresas a regulamentações externas e políticas internas com o propósito de assegurar os recursos da rede de ameaças em evolução” (FALSARELLA, 2010).

Soluções de NAC são basicamente ferramentas que asseguraram o controle de acesso a todos os dispositivos onde diretamente ou indiretamente acessam a rede. Implementações do NAC bem arquitetadas podem gerenciar facilmente diferentes níveis de usuário como, por exemplo, usuários confiáveis (que fazem parte de um determinado grupo da rede corporativa de uma empresa) ou usuários convidados (pessoas ou determinados dispositivos externos que eventualmente conectam a rede). Este controle é baseado em critérios de políticas de segurança como identificação do usuário, tipo ou “estado” do dispositivo, dia e hora de acesso, departamento. Uma arquitetura do NAC combinada aos critérios de políticas bem segmentadas torna o sistema em um contexto geral mais robusto alavancando uma série de funções importantes, na qual classificamos como **DAAAR** (*Detect, Authenticate, Assess, Authorize, Remediate).* Estas funções permitem as organizações de TI implantarem rapidamente o NAC e o mais importante, de uma forma progressiva alinhando com as necessidades do negócio.

Em uma rede corporativa típica, 30 a 50 por cento de todos os dispositivos finais são desktops ou laptops. O maior percentual consiste em um conjunto diversificado de dispositivos conforme mostra o gráfico abaixo:

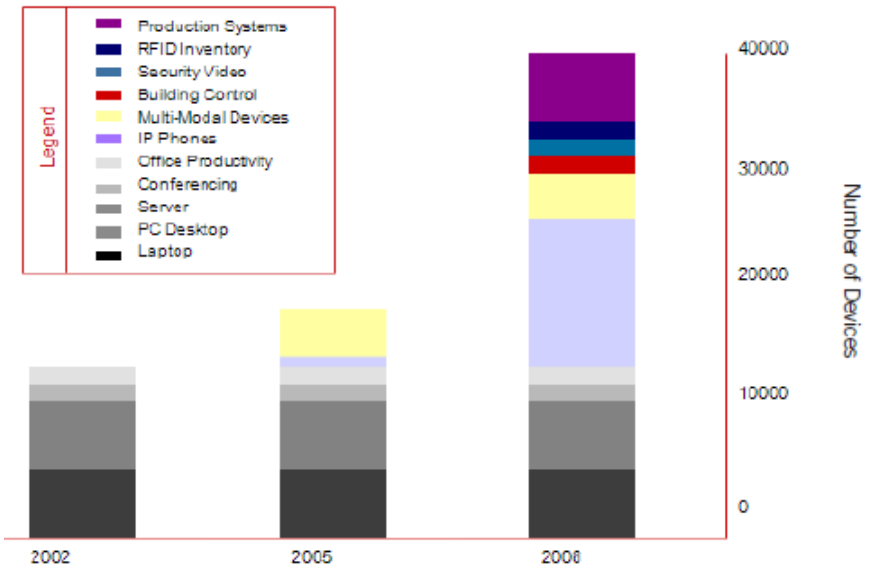

Figura 5. Representação gráfica de negócio as tecnologias NAC
Fonte: Enterasys – *Understanding Network Access Control*, 2008.

2.6 CONTROLE DE IDENTIFICAÇÃO (identidade do usuário)

Com o controle de identidade do usuário é possível criar filtros de entradas nas solicitações realizadas pelos dispositivos da rede. Uma vez que estes dispositivos alcancem o sistema de segurança, eles passam pelo processo de autenticação no qual são verificados para realmente saber quem eles dizem que são então o sistema de segurança solicita as provas do usuário, esta evidência e nomeada como credencias do usuário ou identidade do usuário. Estas identidades podem ser um tipo de acesso, tipo de dispositivo, localidade, tipo de autenticação e assim por diante.

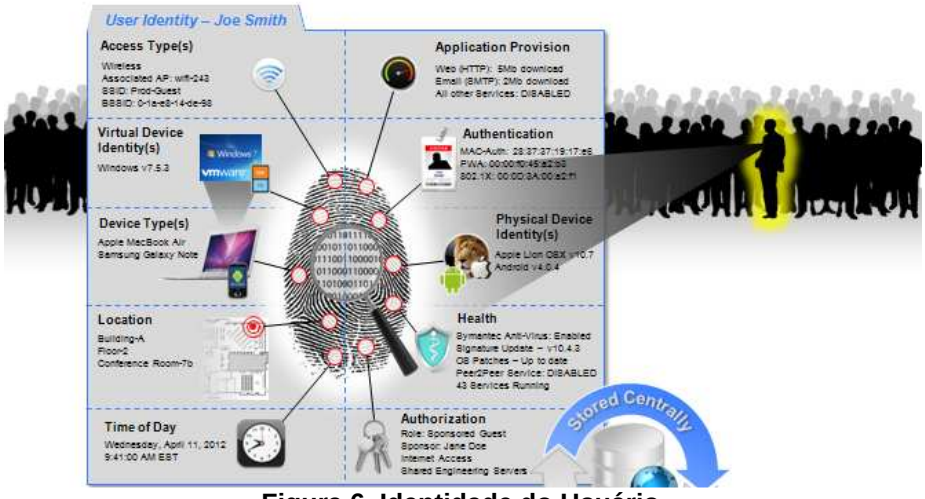

Figura 6. Identidade do Usuário
Fonte: Enterasys – *Smartphones and Tablets in the Enterprise* - 2011.

2.7 TIPO DE DETECÇÃO DO DISPOSITIVO

O tipo de detecção do dispositivo é o primeiro passo fundamental para o conjunto de medidas de segurança adotadas pelo NAC. A detecção de novos dispositivos ao longo da rede com o recurso de detectar o tipo de dispositivo permite o processo de detecção de registro do equipamento no ambiente de rede. Além das funções padrões do NAC, como autenticação, autorização, avaliação e remediação a ferramenta permite a capacidade de detecção por perfil (por exemplo, detecção de tipo de dispositivo) e controlar qualquer tipo de usuário final conectado a infraestrutura local. O NAC detecta automaticamente estes novos dispositivos e atribui a um perfil com base no conjunto de credenciais validadas configuradas como regras. Abaixo mostra uma pequena demonstração de como as informações de detecção e identificação dos dispositivos são apresentados no NAC.

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

Figura 7. Diferentes tipos de dispositivos detectados pelo NAC
Fonte: Enterasys – *Smartphones and Tablets in the Enterprise* - 2011.

Após a detecção do dispositivo e perfil, os recursos de acesso são facilmente gerenciáveis. Por exemplo, criar uma regra para dispositivos IPhone que mesmo o usuário (interno ou externo) onde credenciais válidas para autenticar na rede pode ter seu acesso limitado, já um notebook corporativo tem uma regra privilegiada e acesso a outros recursos. Os recursos utilizados para detectar o IPhone e o notebook são os mesmos, muda apenas a maneira como o sistema foi customizado. A infraestrutura de um modo geral fica totalmente automatizada e dinâmica, reduz custos operacionais permitindo a convergência a fim de garantir a segurança lógica no local.

3 ESTUDO DE CASO

Este capítulo apresentará parte de uma solução implantada na rede do Boticário – São José dos Pinhais envolvendo o conceito BYOD.

3.1 CENÁRIO

A instalação e configuração inicial da solução *Mobile IAM* (BYOD) dos equipamentos de rede legado da Enterasys Networks na rede do Boticário será com configuração homogênea de políticas no ambiente cabeado e sem fio.

O objetivo para aplicação do BYOD é proporcionar maior visibilidade quanto ao acesso à rede do Boticário, fornecendo informações que permitam o registro de acessos em conformidade com normas de segurança como PCI DSS 10.2.5 (*"Use of identification and authentication mechanism"*).

3.2 TOPOLOGIA UTILIZADA

Com a utilização da ferramenta *Mobile IAM (Identity and Access Management)* será implementado um controle de acesso preventivo, com a utilização de mecanismos de controle que possam garantir a implementação das definições de acesso descritos na política de segurança do Boticário de forma efetiva e automatizada. Com modelo preventivo de segurança chamado RBAC (*Role-Based Access Control*), será possível fazer o controle de acesso a rede fornecendo conectividade com as permissões de acordo com o perfil de cada usuário que se conecte a rede.

3.3 DIAGRAMA DE CONTROLE DE ACESSO RBAC

O modelo de acesso (RBAC), que será demonstrado a seguir tem por objetivo fornecer conectividade baseada no perfil de cada usuário/equipamento conectado a rede do Boticário. Este modelo simplifica o controle de acesso à rede pela aplicação de restrições, QoS e segmentação do acesso levando em

consideração a necessidade de acesso para cada perfil definido pela área de segurança da empresa.

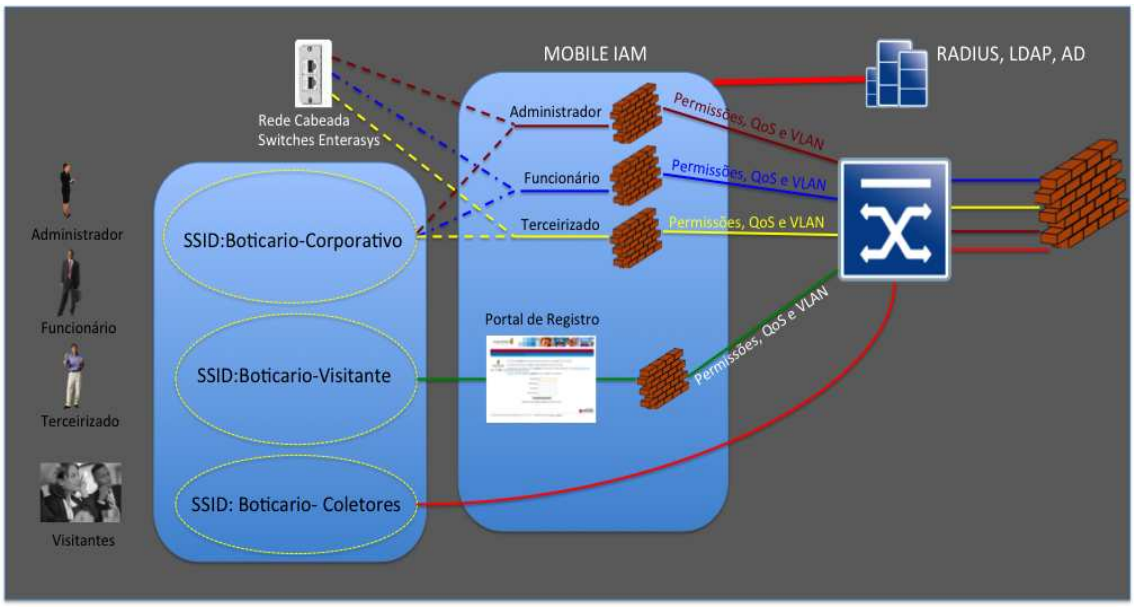

Figura 8. Diagrama RBAC - Boticário
Fonte: Autoria Própria.

3.4 DESCRIÇÃO DAS FERRAMENTAS UTILIZADAS

Atualmente o cliente já possui o ambiente com os pré-requisitos para implantação do BYOD, as configurações iniciais da solução serão realizadas no equipamento *Network Access Control* (*NAC-Manager*) em conjunto o NAC Gateway Virtual Appliance adquiridos pelo cliente, proporcionando meios para o gerenciamento seguro baseada em políticas para dispositivos móveis e cabeados conectados em equipamentos Enterasys.

3.5 CLASSIFICAÇÃO DOS DISPOSITIVOS

Todos os dispositivos da rede LAN passarão pelos requisitos do NAC, inicialmente a detecção, em seguida será avaliado as credenciais do usuário, com base nas credenciais do usuário lhe será concedido o perfil destinado.

	Perfil	Descrição	Restrições
1	**Computadores**	Fornecer credenciais de acesso a rede para os computadores do domínio;	O perfil deve ter acesso a rede com restrições de somente a recursos de atualização de antivírus, SWUS, e fornece acesso para o helpdesk;
2	**Administrador**	Fornecer credencial a nível Administrador para o ambiente de rede;	Perfil sem restrições de acesso a rede com objetivo de permitir a administração da rede e troubleshooting;
3	**Usuario**	Fornecer credencial de acesso para os usuários corporativos;	
4	**Usuario Avancado**	Fornecer credencial de acesso para usuários VIPs;	Quase todas as funções de administrador com algumas restrições;
5	**Visitante**	Fornecer credencial de acesso para visitantes internos e externos	
6	**Impressora**	Fornecer credencial de rede para Impressoras do domínio baseado em MAC	
7	**Dispositivos**	Fornecer credencial de rede para dispositivos ligados à rede baseado em MAC;	
8	**Telefones**	Fornecer credencial de rede para Telefones IP do domínio baseado em MAC;	
9	**Não Autenticado**	É o perfil padrão para usuários não autenticados no domínio.	
10	**Quarentena**	Perfil utilizado para usuários em não conformidade a rede;	

Figura 9. Exemplo - Perfis de Acesso aos dispositivos
Fonte: Autoria Própria.

Para o ambiente Wireless será configurado um único *SSID* corporativo (*Service Set IDentifier*) que deve classificar e aplicar políticas de acesso baseado em dispositivo e usuário, bloqueando ou permitindo acesso a recursos corporativos com as definições estabelecidas pelos departamentos de Segurança da Informação.

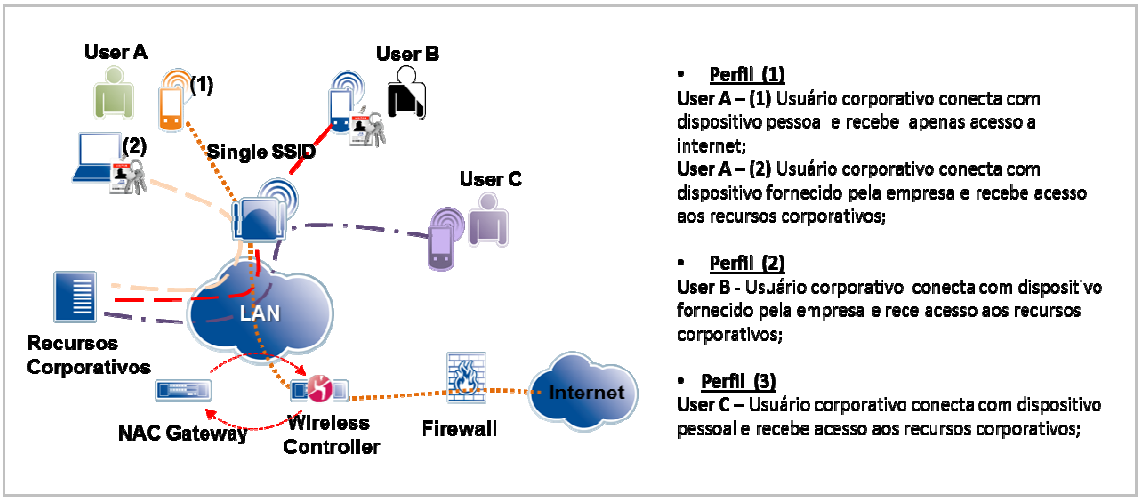

Figura 10. Exemplo – SSID única dispositivos corporativos sem fio
Fonte: Autoria Própria.

3.5.1 EXEMPLO – ACESSO VISITANTES

Usuários visitantes não fazem parte da rede corporativa portando será configurado um SSID Visitante exclusiva que deve classificar e aplicar políticas de acesso baseado em dispositivo e usuário conforme as definições estabelecidas pelos departamentos de Segurança da Informação.

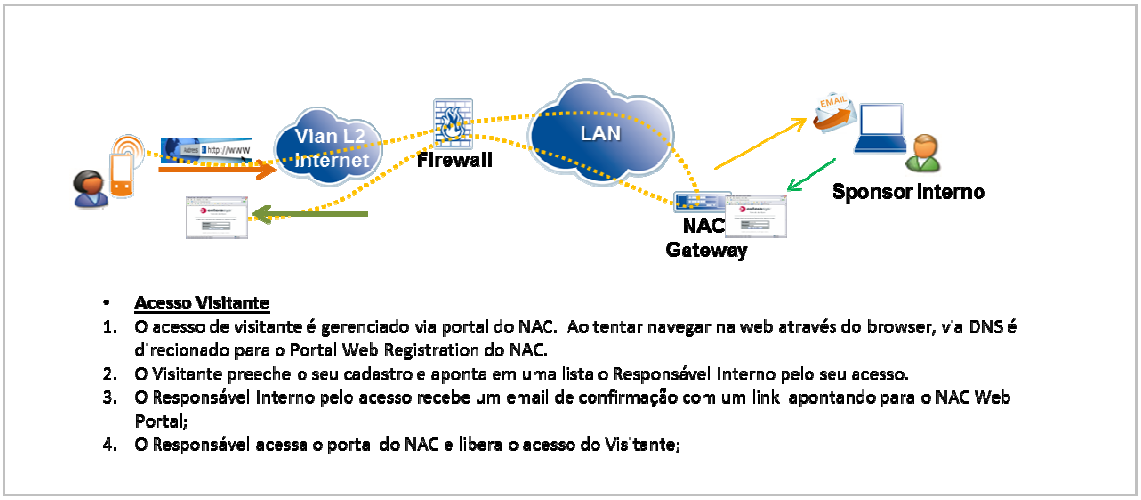

Figura 11. Exemplo – SSID para acesso de visitantes
Fonte: Autoria Própria.

O Boticário deve determinar como funcionará o fluxo de autorização dos visitantes. Dentre as várias opções possíveis foi definido durante fase de homologação que o visitante irá preencher um formulário com seus dados pessoais e um colaborador do Boticário terá permissão de dar autorização de acesso por meio de site WEB.

Abaixo segue exemplo do registro via portal que foi customizado para permitir ao grupo entender como será disponibilizado o acesso. Todo o texto poderá ser traduzido para português de acordo com definição a ser entregue pelo grupo Boticário. A customização poderá ser feita no texto, e figuras com posição fixada no portal. Não será possível modificar o layout do portal:

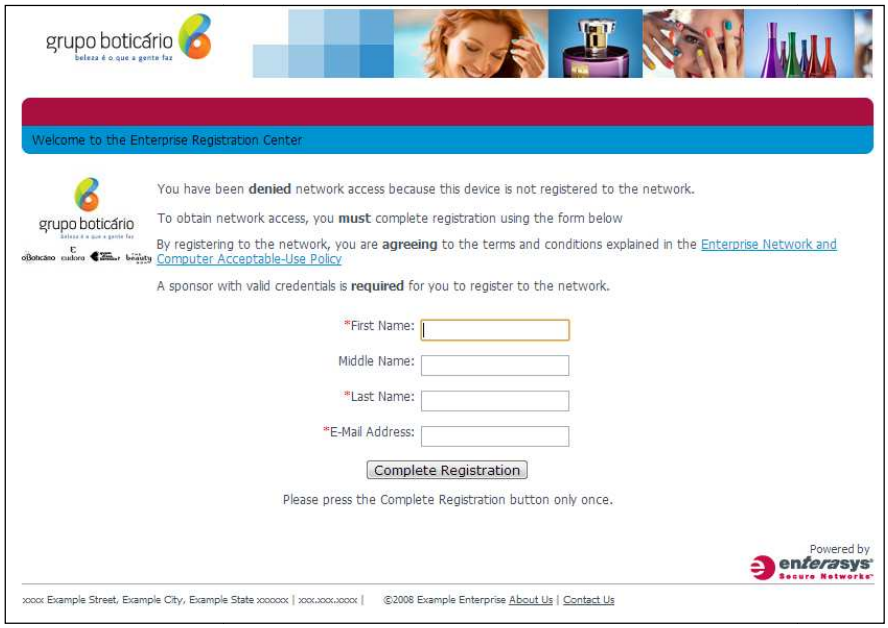

Figura 12. Exemplo – Registro de acesso via portal
Fonte: Intranet Boticário.

3.6 PERMISSÕES DE ACESSO

As definições de acesso e regras do portal serão definidas pelo departamento de Segurança da Informação, conforme exemplo abaixo:

- Grupo do AD (Active Directory) que terá permissão de administração dos visitantes no Mobile IAM;
- Grupo do AD (Active Directory) que terá permissão de autorizar acesso à rede de visitantes do Boticário;
- Termo de uso aceitável para inclusão no portal;
- Texto e imagens a serem utilizadas no portal com objetivo informar e colocar características visuais do Boticário;

Formas possíveis de implementar o portal de visitantes:

- Registro com autorização um usuário responsável pelo visitante;

- Registro com acesso liberado de forma automática com envio de e-mail ao administrador para conhecimento;
- Autenticação de usuário de base local do Mobile IAM;
- Autenticação de usuário com conta do Active Directory;
- Registro com obrigatoriedade de numero de celular para recebimento de SMS (*Short Message Service*) com conta de usuário e senha para acesso seguro através do SSID corporativo e segmentado na rede de visitantes. Esta opção exige que o Boticário tenha um gateway de SMS com alguma operadora de celular;

Com objetivo de reduzir necessidade de indisponibilidade de serviços no Boticário, será necessário criação de novas redes(VLANS, Endereços IPs, etc) para que o serviço atual não tenha impacto e não crie necessidade de janelas de manutenção no período da madrugada;

3.7 RISCOS INICIAIS IDENTIFICADOS

A aplicação do conceito BYOD, como toda e qualquer implantação, está sujeita a riscos, abaixo foram observados alguns fatores de risco que podem interferir na implantação:

- As definições das políticas de acesso para cada tipo de usuário/dispositivo dependem da validação e aprovação por parte do Boticário;

- O cadastro dos dispositivos autenticados via MAC através do NAC depende de lista fornecida pelo cliente, ou seu cadastro posterior deve ser feito pelo Boticário.

- A definição e configuração de mecanismo de filtro de conteúdo e topologia para acesso o SSID de visitante utilizando o Portal Web do NAC depende do envolvimento de recursos do Boticário (WebSense ou InetHotel ou Firewall).

3.8 TESTES E RESULTADOS

Como o projeto de estudo trata-se apenas do escopo para implantação no cliente, a seguir são demonstrados alguns exemplos do conceito BYOD aplicado em experiências anteriores de projetos implantados pelo aluno, é possível ter ideia do ambiente com a integração de todas as ferramentas utilizadas.

Foi utilizado para demonstração dos resultados do BYOD a ferramenta *OneView* da Enterasys, na qual realiza o gerenciamento das ferramentas da rede *LAN/WAN* em uma única plataforma.

Configurações relacionadas ao BYOD são acessíveis através do Painel *End-Systems*, informações como *ip* do dispositivo, sistema operacional e nome do usuário são facilmente apresentados. Estes itens só estarão visíveis após configuração das regras no NAC.

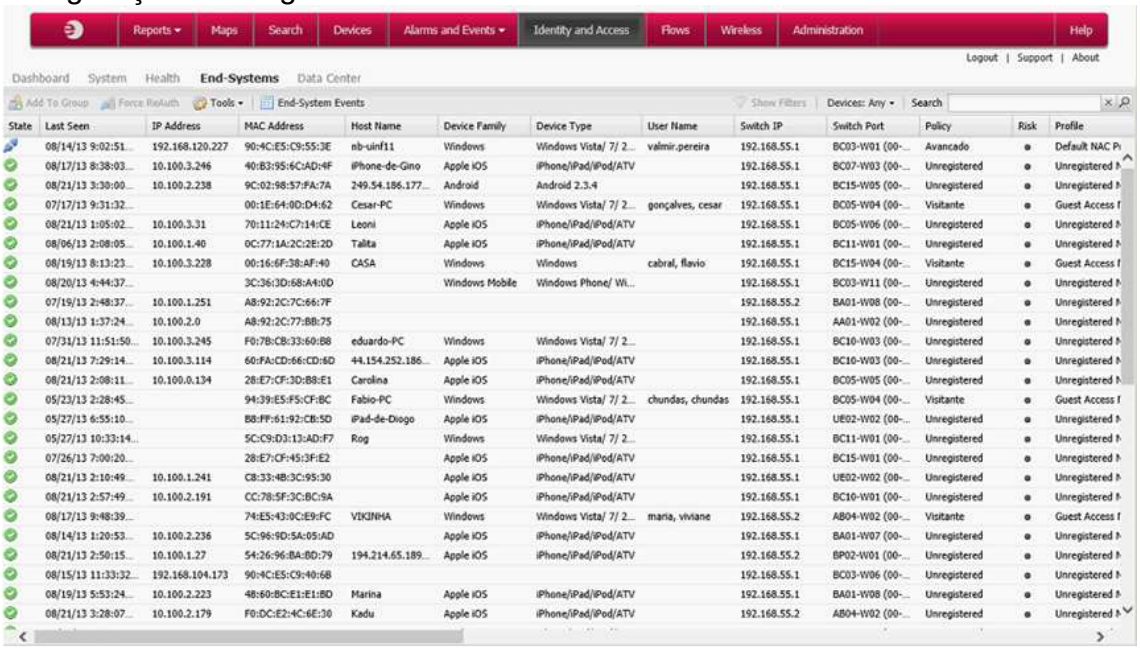

Figura 13. Painel visual de dispositivos finais conectados a rede
Fonte: Autoria Própria.

Outra funcionalidade interessante é o Painel de instrumentos ou *Dashboard* onde graficamente são apresentados os resultados por zonas. Quantidade de dispositivos que não foram aceitos pela rede, os perfis de acesso (perfis não registrados, convidado, permitidos e o ultimo nível de quarentena). Dados como sistema operacional do dispositivo (*Windows, Linux, Apple IOS, Android*) e tipo de autenticação (*802.1x,MAC, convidado)* são visualizados nesta sessão. O painel é modelado de acordo com refinamento dos dados configurados na solução, quanto mais específico, mais preciso o nível de informação da rede.

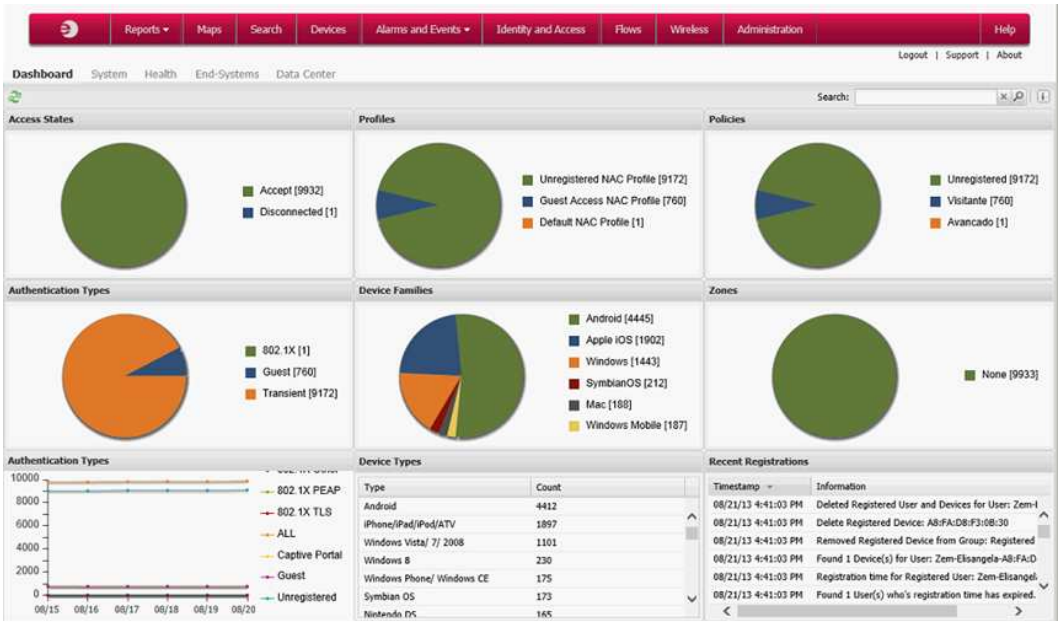

Figura 14. Painel de Instrumentos (Dashboard)
Fonte: Autoria Própria.

Finalmente um dos recursos mais valorizados de toda a integração das ferramentas é o painel visão global ou *Overview,* demonstra de forma visual como este dispositivo está conectado a rede, no exemplo abaixo um dispositivo móvel (IPhone) conectado a rede *wireless* (dispositivo *Access-point)* que por sua vez gerenciado pelo *Wireless Controller.* Nesta seção é possível pesquisar todas em detalhes todas as informações entre os dispositivos conectados (usuário de acesso do IPhone, SSID em que o dispositivo está conectado, qual o método de autenticação utilizado, etc.)

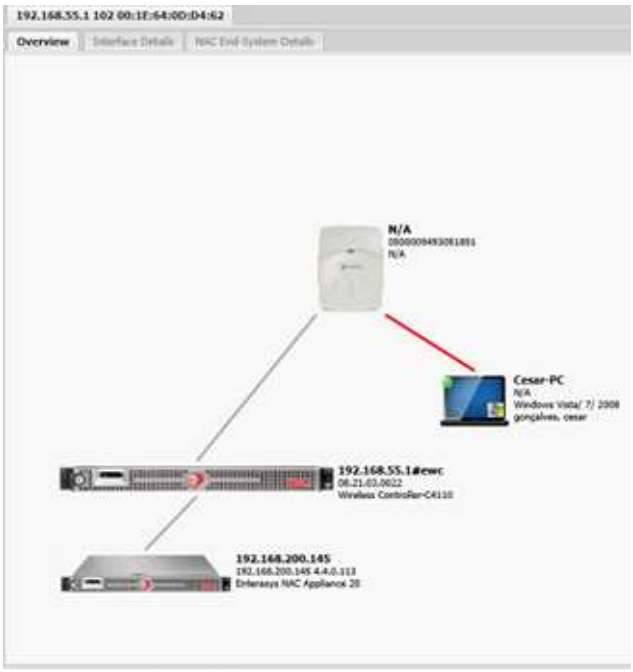

Figura 15. Painel de Visão Global (Overview) – Exemplo (computador)
Fonte: Autoria Própria.

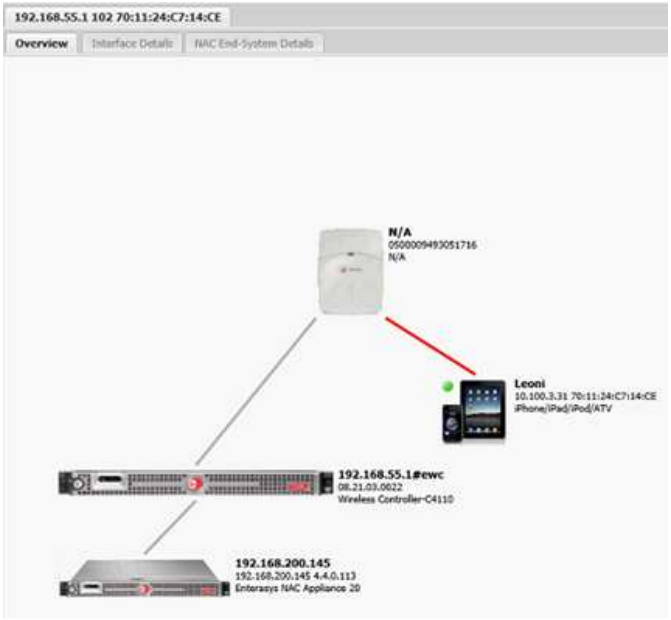

Figura 16. Painel de Visão Global (Overview) – Exemplo (IPad)
Fonte: Autoria Própria.

Todas as ferramentas foram apresentadas ilustrativamente apenas para demonstração do conceito BYOD.

4 CONSIDERAÇÕES FINAIS

Nos últimos anos a tecnologia da informação vem demonstrando maior influência no mundo corporativo com novos métodos e mecanismos de segurança em redes. Tal fator levou os departamentos de TI a buscar novas formas de proteger seus ambientes devido ao crescimento nas redes corporativas de médio e grande porte. Podemos afirmar que a consumerização agrega diferenciais competitivos, pois os colaboradores passaram a utilizar seus equipamentos pessoais para realizar tarefas ligadas ao trabalho que até então só poderiam desempenha-las no próprio local. Esta liberdade tem seu lado positivo, mas também aspectos negativos. Do ponto de vista do colaborador tudo é transparente, já para o ambiente corporativo um “quebra-cabeça” a montar.

Aplicar políticas de segurança adequadas, estipular regras e conscientizar os colaboradores sobre os riscos do mau uso de seus equipamentos no ambiente corporativo são medidas preventiva contra vazamento de informações de negócio ou até mesmo pessoal. No estudo de caso na implantação do BYOD foi utilizada como exemplo a separação por perfis de acesso utilizando a ferramenta de controle de acesso (NAC), onde um determinado conjunto de regras é atrelado a um perfil e qualquer dispositivo que se conecte a rede (corporativo ou não) seja devidamente identificado em um destes perfis. Através da aplicação de conceitos e ferramentas de segurança da informação adequadas pode-se sim tornar o ambiente propício ao BYOD.

Por fim, as empresas com o tempo tendem a aderir a este movimento, precisam apenas encontrar uma maneira de incorporá-la a todos os dispositivos, de forma a tornar o ambiente com nível de segurança apropriado sem por em risco a continuidade do negócio.

REFERÊNCIAS

COCCHI, Debora. MORAES, Eduardo A. ***Política de Segurança para aplicação BYOD***. Disponível em <http://www.profissionaisti.com.br/2013/06/politica-de-seguranca-para-aplicacao-byod/> Acesso em 07/07/2013, 18:28

CISCO IBSG. ***BYOD: uma perspectiva global***. Disponível em <http://www.cisco.com/web/about/ac79/docs/re/byod/BYOD_Horizons_Global_PTBR.pdf> Acesso em 07/07/2013, 18:32

CISCO SYSTEMS. ***Article - Cisco Ends Investment in Cius Tablet in Face of BYOD Cloud***. Disponível em <http://go.galegroup.com.ez48.periodicos.capes.gov.br/ps/i.do?id=GALE%7CA290783072&v=2.1&u=capes58&it=r&p=AONE&sw=w> Acesso em 20/07/2013, 10:35

COMPUTER WORLD. ***Como demitir num mundo BYOD***. Disponível em <http://www.computerworld.com.pt/2013/07/02/como-demitir-num-mundo-byod/> Acesso em 07/07/2013, 18:19

ENTERASYS. ***Understanding Network Access Control***. Disponível em < https://extranet.enterasys.com/downloads/Pages/dms.ashx?download=1584b35f-08ce-4108-a07e-65b6c65659d1> Acesso em 13/07/2013, 09:15

ENTERASYS. ***Smartphones and Tablets in the Enterprise - Managing BYO Device Programs***. Disponível em < http:// http://www.enterasys.com/company/literature/byo-device-programs-sab.pdf> Acesso em 13/07/2013, 09:15

FALSARELLA, Douglas. ***NAC: Redes mais seguras***. Disponível em < http://imasters.com.br/artigo/17375/redes-e-servidores/nac-redes-mais-seguras/> Acesso em 30/07/2013, 22:35

FERRAIOLO, David F. CUGINI, Janer A. ***Role-Based Access Control (RBAC): Features and Motivation***. Disponível em < http://www.cs.unibo.it/~montreso/master/materiale/ac/rbac.pdf> Acesso em 16/08/2013, 17:08

INTEL CORPORATION. ***Research - Insights on the Current State of Byod***. Disponível em <http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/consumerization-enterprise-byod-peer-research-paper.pdf> Acesso em 30/07/2013, 22:40

KANESHIGE, Tom. ***Cinco Custos ocultos do BYOD*.** Disponível em < http://cio.uol.com.br/gestao/2012/04/12/cinco-custos-ocultos-do-byod> Acesso em 05/08/2013, 19:55

MELLO, Andre. ***BYOD chega à maioridade com ajuda das soluções MAM***. Disponível em <http://www.baguete.com.br/artigos/1232/andre-mello/10/05/2013/byod-chega-a-maioridadecom-ajuda-das-solucoes-mam> Acesso em 17/07/2013, 20:21

NASCIMENTO, Marcelo. ***A tendência do BYOD***. Disponível em <http://www.portalgsti.com.br/2013/06/BYOD-tendencia.html> Acesso em 17/07/2013, 22:08

OLHAR DIGITAL. ***Bring your Own Device: que tal levar seus próprios dispositivos para o trabalho?*** .Disponível em <http://olhardigital.uol.com.br/produtos/mobilidade/noticias/bring-your-own-device-que-tal-levar-os-proprios-dispositivos-para-trabalhar> Acesso em 17/07/2013, 20:23

OLTSIK, Jon. ***White Paper - A Roadmap for BYOD Adoption***. Disponível em < https://extranet.enterasys.com/downloads/Pages/dms.ashx?download=f03c9248-defd-43ec-8020-71211cd8cfff > Acesso em 03/08/2013, 14:35

PCI Security Standards Council. ***Requirements and Security Assessment***. Disponível em < https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf> Acesso em 06/08/2013, 21:15

PINHEIRO, P. Patricia. ***Como Fazer Uma Política de BYOD?*** . Disponível em <http://www.pppadvogados.com.br/Publicacoes.aspx?v=1&nid=1285> Acesso em 17/07/2013, 22:21

SILVEIRA, S. Vinicius ***BYOD: a implantação inteligente é o novo desafio***. Disponível em <http://revistaapolice.com.br/2013/06/byod-a-implantacao-inteligente-e-o-novo-desafio/> Acesso em 17/07/2013, 22:00

STALLINGS, William. ***Criptografia e Segurança de Redes*.** Ed Prentice Hall, 2005