UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM TECNOLOGIA
MBA EM GESTÃO DE SERVIÇOS DE TELECOMUNICAÇÕES

WAGNER DOBZINSKI SANTOS

POLÍTICAS DE USO E SEGURANÇA DA INFORMAÇÃO: um estudo sobre aplicação byod - bring your own device

MONOGRAFIA

CURITIBA
2017

WAGNER DOBZINSKI SANTOS

POLÍTICAS DE USO E SEGURANÇA DA INFORMAÇÃO: um estudo sobre aplicação byod - bring your own device

Monografia apresentada como requisito parcial para a obtenção do grau de Especialista em Gestão de Serviços de Telecomunicações, do Programa de Pós-Graduação em Tecnologia. Da Universidade Tecnológica Federal do Paraná. Área de Concentração: Redes de Computadores.

Orientador: Prof. Alexandre Miziara

CURITIBA
2017

AGRADECIMENTOS

Agradeço a Deus em primeiro lugar por ajudar em cada desafio no dia a dia.

Aos Professores(as) da UTFPR que nos repassaram o seu conhecimento nesse período do curso.

Em especial um agradecimento ao Professor e cordenador do curso Alexandre Miziara que foi o meu orientador e a Professora Rosangela Stankowitz me auxiliaram na elaboração dessa monografia.

RESUMO

SANTOS, Wagner Dobzinski. Politícas de uso e segurança da informação para aplicação BYOD – Bring Your Own Device. 2017. 46p. Monografia de Especialização em Gestão de Serviços de Telecomunicações - Universidade Tecnológica Federal do Paraná. Curitiba, 2017.

A presente monografia tem como objetivo de analisar a modalidade chamado BYOD (Bring Your Own Device). É uma tecnologia que envolve serviços, políticas e tecnologias que viabilizam aos funcionários desempenhar atividades profissionais utilizando seus próprios equipamentos, como smatphones, tablets ou notebooks. Essa mobilidade facilita na produtividade e agilidade na execução das tarefas.
Trata-se de um conceito mundial que vem ganhando força entre as organizações, chama a atenção das empresas tanto pelo ganho de produtividade quanto pela redução em investimentos em equipamentos. Para isso foi realizado um estudo sobre BYOD, analisando principais tecnologias para manter a segurança dos dados corporativos, e os cuidados com a utilização de dispositivos móveis, os desafios de segurança que a empresa precisa ter ao implantar a modalidade, foi utilizada uma metodologia qualitativa de natureza exploratória e descritiva para conclusão do trabalho. Os principais resultados mostram que uma política de segurança BYOD bem implantada o risco de perda dos dados corporativos são minimos.

Palavras-chave: Políticas de Segurança. BYOD. Dispositivos Móveis. NAC (Network Access Control). Virtualização.

ABSTRACT

SANTOS, Wagner Dobzinski. Politícas de uso e segurança da informação para aplicação BYOD – Bring Your Own Device. 2017. 46p. Monografia de Especialização em Gestão de Serviços de Telecomunicações - Universidade Tecnológica Federal do Paraná. Curitiba, 2017.

This monograph aims to analyze the modality called BYOD (Bring Your Own Device). It is a technology that involves services, policies and technologies that enable employees to perform professional activities using their own equipment, such as smatphones, tablets or notebooks. This mobility facilitates productivity and agility in the execution of tasks.
This is a worldwide concept that has been gaining strength among organizations, it draws the attention of companies both for the gain of productivity and for the reduction in investments in equipment. For this, a study was carried out on BYOD, analyzing the main technologies to maintain the security of corporate data, and the care with the use of mobile devices, the security challenges that the company must have when implementing the modality, was used a qualitative methodology of exploratory and descriptive nature to complete the work. The main results show that a BYOD security policy well implemented the risk of loss of corporate data are minimal.

Keywords: Security Policies. BYOD. Mobile Devices. NAC (Network Access Control). Virtualization.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

BYOD Bring Your Own Device é a nova tendência do mercado de trabalho. A sigla significa “traga o seu próprio dispositivo” e dá aos funcionários da empresa a oportunidade de utilizar os seus próprios aparelhos para acessar dados e informações da companhia. Com isso, o funcionário tem liberdade para utilizar a tecnologia que mais lhe convém, proporcionando um ambiente de trabalho mais confortável.

NAC Network Access Control ou Controle de Acesso à Rede é um componente importante de uma solução de gerenciamento de segurança abrangente.

MDM Mobile Device Management é normalmente implementado com o uso de um produto de terceiro que possui recursos de gerenciamento para fornecedores particulares de dispositivos móveis.

MAM Mobile Application Management Gerencia totalmente aplicativos utilizados no ambiente de trabalho, sejam eles internos ou externos um dos módulos que compõem uma solução completa de EMM (Enterprise Mobility Management, ou gestão da mobilidade corporativa) é o MAM (Mobile Application Management, ou gestão de aplicativo móvel)

DAAS Desktop as a Service é mais um modelo de utilização de recursos de Tecnologia da Informação, onde é possível substituir o modelo tradicional de aquisição de produtos, pela contratação de serviços, ou seja, ao invés de você adquirir um desktop (hardware) e softwares (sistema operacional, softwares de proteção, softwares de produtividade etc.)

RBAC Role Based Access Control ajuda você a controlar quem pode realizar as várias tarefas do Intune em sua organização e a quem essas tarefas se aplicam.

PHISHING é uma maneira desonesta que cibercriminosos usam para enganar você a revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Eles fazem isso enviando e-mails falsos ou direcionando você a websites falsos.

LTE Long Term Evolution é um padrão de redes celulares que permite banda larga móvel com velocidades de conexão de até 100 Mbps, possibilitando uma maior abrangência de comunicações de voz e transferência de dados.

PIN Personal Identification Number é um código de segurança diferente da senha de acesso a sua conta Bcash. É um código de até 10 dígitos que o usuário cadastra no momento em que realiza o primeiro login em sua conta. O PIN é utilizado para confirmar algumas operações tais como: transferência de dinheiro, pedidos de saque, alteração de e-mail entre outros garantindo que apenas você tem acesso à sua conta Bcash.

AES Advanced Encryption Standard é uma primitiva criptográfica destinada a compor sistemas de cifragem e decifragem simétrica (mesma chave para cifrar e decifrar). É uma cifra de bloco, ou seja, opera em blocos de tamanho fixo (128 bits, ou 16 bytes).

BLOWFISH é uma cifra simétrica de blocos que pode ser usado em substituição ao DES, algoritmo que possuía em torno de 19 anos de uso, e era vulnerável a ataques por força bruta devido ao tamanho de sua chave (56 bits).

Sumário

1 INTRODUÇÃO

As empresas buscam maior produtividade nas tarefas que são passadas aos funcionários, o metodo BYOD, desde que bem implementado na organização facilita na rapidez para executar uma tarefa, além disso reduz o custo com equipamentos e deixa os funcionários mais interessados em desenvolver e concluir as atividades utilizando os próprios dispositivos móveis.

Através de *Home Office* ou clientes externos, mostrando os cuidados com a proteção dos dados no ambiente corporativo, e as politicas de segurança envolvidas com essa utilização dos dispositivos com informações importantes, um exemplo que pode ser citado é mostrado pela DELL/KACE, este dispositivo considerou mais de 1.500 CIOs, destes, 48% responderam que não autorizaram a prática de BYOD.

Por entenderem que apenas confiar ou simplesmente proibir não seja a alternativa mais eficaz para a mitigação dos riscos, porém, concordam que é necessário fazer mudanças na cultura, infraestrutura, suporte, custos, políticas, segurança e governança dentro das corporações para a implantação desta prática.

Como o fenômeno da consumerização, veio uma nova forma de conciliar diversas tarefas em um único gadget, desde acesso à internet, e-mails, e ferramentas Office com o intuito de aumentar a flexibilidade no trabalho diversas práticas, como a do Bring your own technology (BYOT), Bring your own phone (BYOP), Bring your own PC (BYOPC), e o Bring your own device (BYOD).

1.1 JUSTIFICATIVA

Com a evolução tecnológica nos últimos anos a necessidade de um gerenciamento de redes corporativas pelo departamento de tecnologia da informação, uma estratégia BYOD bem implantada na organização além de crescimento e produtividade, contribui para redução de custos, esse estudo não tem a finalidade de mostrar apenas os benefícios decorrentes do uso de smartphones e tablets no ambiente empresarial.

Tem o objetivo de apresentar também, quais são os possíveis problemas e riscos que a utilização dessa tecnologia pode ocasionar, assim como os desafios

na área de segurança no uso desses dispositivos móveis, 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.

1.2 PROBLEMA

O movimento BYOD tornou a missão da área de segurança corporativa muito mais complexa, entende-se que este conceito de proteção ao usuário inova na medida em que foca nos sérios desafios que surgem com a utilização de dispositivos diversos, que vão e vêm de outros ambientes para a empresa, mudando as necessidades de proteção e aumentando a complexidade das ameaças.

O que exige um cuidado diário por parte da área de segurança, o conceito também agrega valor às organizações em termos de redução de custos com equipamentos, flexibilidade de gerenciamento e eficácia na proteção dos seus usuários com os dispositivos.

Este estudo busca responder a seguinte pergunta de pesquisa: A implantação de políticas de uso e segurança do conceito BYOD nas empresas é seguro?

1.3 OBJETIVOS

O objetivo geral deste trabalho é estudar e analisar a modalidade chamada BYOD (Bring Your Own Device) no ambiente corporativo e home office abordando os cuidados e a política de segurança envolvidos na utilização de dispositivos móveis pessoais, contendo informações confidenciais da empresa, e como manter as informações em segurança.

1.3.1 OBJETIVO GERAL

O objetivo geral deste trabalho é estudar e analisar a modalidade chamada BYOD (Bring Your Own Device) no ambiente corporativo e home office.

1.3.2 OBJETIVOS ESPECÍFICOS

I) Identificar os fatores positivos e negativos na utilização do BYOD.

II) Averiguar os riscos por mau uso de dispositivos móveis das organizações.

III) Levantar as Políticas de uso e segurança da informação das organizações.

IV) Mapear como as organizações utilizam as criptografias.

1.4 ESTRUTURA DO TRABALHO

A monografia é constituída por 5 capítulos. O capítulo 1 trata da parte introdutória, abordando o tema, objetivos e desenvolvimento, e a estrutura da monografia também são discutidos nesta primeira parte.

Com relação ao capítulo 2 trata-se do referencial teórico do projeto. Questões relacionadas ao BYOD, dispositivos móveis, 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.

No terceiro capítulo são apresentados os procedimentos metodológicos para o estudo com as ferramentas escolhidas a pesquisa. No quarto capítulo são apresentadas as ferramentas para minimizar os riscos na utilização de dispositivos móveis.

O quinto capítulo são feitas as conclusões finais sobre todo o estudo realizado do Bring your own device, por último as referências utilizadas para desenvolvimento da monografia.

2 REFERENCIAL TEORICO

2.1 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

As regras e políticas são criadas para que o funcionário dentro da organização possa ter consciência de que a informação obtida dentro da organização é um ativo de valor para agregar o negócio, devido a isso, devem estar

asseguradas de maneira rigorosa, cabe ao funcionário à responsabilidade de assegurar a informação que lhe é transmitida.

Segundo Beltran (2016), a política se aplica a organização com intuito de regrar atividades e normas desenvolvidas para os colaboradores, estas devem ser de conhecimento de todos que trabalham na organização, ser de fácil entendimento e claras, para que isso ocorra, a política deve estar alinhada aos objetivos da organização.

Recebido ou dificultar a obtenção de prova de que tal pessoa cometeu a fraude, recomenda-se que o monitoramento seja efetuado para todos os setores, independentemente de sua hierarquia e que este seja realizado por uma equipe especializada, replicando ao gerente ou dono da empresa seu resultado, sem alterações, furtos e fraudes podem ocorrer a qualquer instante dentro da organização.

Podendo tomar grande proporção e repercussão, causando danos à organização, em relação às fraudes, estas podem ocorrer por vários motivos, porém os de maiores destaques são: fraqueza no controle, oportunidade, necessidade e motivação, no caso de necessidade, o maior fator é dinheiro, levando o funcionário a fraudar a organização.

Ainda segundo Beltran (2016), roubando informações ou equipamentos, gerada pela curiosidade, acontece em casos que, por descumprimento das políticas de segurança, alguma informação fica exposta a pessoas não autorizadas e essas, por motivação, onde colaboradores de má índole se veem propícios a tirar vantagens dessas falhas.

Utilizando sua inteligência para obter lucros com as informações roubadas sem tanto esforço, a política ajuda definir quais as melhores estratégias, processos e padrões que deverão ser utilizados, após esses aspectos serem determinados.

De acordo com Beltran (2016), também é necessário direcioná-los as ações para tomada de decisões, a fim de que se possa atingir o objetivo esperado, uma política fará com que a organização consiga assegurar todas suas informações tomando a diretriz correta, os ataques maliciosos também ocorrem devido às vulnerabilidades que, ao contrario das ameaças, é explorada.

Trata-se da fragilidade, por exemplo: com a falta de treinamento, que seria a vulnerabilidade, as informações podem se perder e, a perda de informações

se torna uma ameaça, o ideal é verificar as vulnerabilidades obtidas nestas ameaças, isso pode ser efetuado pelo controle, o mesmo que foi efetuado para verificar ameaças, neste caso, em sua segunda etapa a organização também pode implementar nas suas políticas de segurança da informação.

Quais são os principais aplicativos a serem utilizados e os principais aplicativos a não serem utilizados através da rede corporativa, as políticas de segurança da informação de uma empresa são formadas geralmente pelo conjunto de políticas mais específicas, uma das principais políticas é a autenticação do usuário (BELTRAN, 2016).

2.2 DISPOSITIVOS MÓVEIS

Capaz de armazenar uma enorme quantidade de dados, os smartphones e tablets estão nas mãos de centenas de milhões de pessoas em todo o mundo, o aumento do consumo desses dispositivos no ambiente corporativo gera um certo medo para empresas, preocupadas com perda de dados e a exposição de informações.

Com todas as senhas armazenadas no seu dispositivo, os criminosos poderiam ter acesso direto às informações pessoais e acesso direto aos sistemas corporativos da empresa, a maior dúvida sobre isso é com relação as políticas que a organização deve adotar, regras e estratégias mesmo sendo dispositivos pessoais ou não.

Os funcionários devem receber instruções quanto ao uso, medidas mínimas de segurança como programas de firewalls, antivírus, e softwares com chaves de criptografia, devem ser aplicadas nos dispositivos que tenham acesso a dados corporativos, mesmo que o departamento de TI faça análises diárias.

É importante ter controle sobre todas as funcionalidades da equipe e que estejam em bom funcionamento, suporte em tempo real de sistemas e softwares e o backup de informações e dados importantes, desta forma é possível proteger o ambiente corporativo de uma empresa.

Visando minimizar as ações de terceiros, para alguns usuários a perda de um dispositivo é quase inevitável pois cada vez menores e mais finos, algumas precauções podem ajudar quando é perdido ou roubado, é possível armazenar dados de uma forma que seja totalmente ilegível se o seu telefone for roubado,

podendo ter acesso remoto ao aparelho, além disto executar vários recursos de proteção e antirroubo.

2.3 SEGURANÇA EM DISPOSITÍVOS MÓVEIS

O número de ameaças à sua segurança cresceu de forma acelerada, de acordo com empresas de segurança, a maioria das infecções em dispositivos móveis é causada por vírus e podem acontecer por causa da falta de atualização dos sistemas operacionais dos aparelhos ou pelo usuário acessar sites não seguros.

De acordo com westcon (2016), os ataques a esses dispositivos podem ocorrer de diversas formas, como através de aplicativos falsos instalados a partir de lojas não oficiais, SMS ou *Phishing*, que é uma técnica de fraude online usada para roubar informações pessoais, senhas de banco, entre outros.

Portanto, tomar algumas precauções podem minimizar esses problemas, como não instalar aplicativos de fontes não conhecidas. Assim, o sistema operacional não se torna vulnerável.

Westcon (2016), ainda explica que há diversos malwares que atacam dispositivos móveis, como o Trojan (Cavalo de Tróia) e são destrutivos, o ataque por Phishing também é muito usado por Hackers, devido ao aumento de número de pessoas que acessam aplicativos pelo smartphone para realizar tarefas do dia a dia, como transações bancárias, compras online e outras.

Mensagens falsas são enviadas por SMS para enganar o usuário, o rootkits, software malicioso, também pode causar diversos danos, como colher informações pessoais da vítima, outra fonte de ameaças aos aparelhos é local com redes Wi-Fi públicas, como shoppings, praças e aeroportos. Pessoas mal-intencionadas podem implantar pontos de acesso Wi-Fi falsos. Segundo Westcon (2016), caso o usuário acesse informações pessoais utilizando essas redes, poderá ter seus dados roubados, a prática de BYOD (Bring Your Own Device) já faz parte da maioria das empresas atualmente e pode trazer vulnerabilidade aos dados da corporação e dos funcionários, se não houver políticas de segurança e controle de acesso.

Caso as empresas não possuam sistemas adequados para alertar os funcionários sobre os riscos à segurança e incentivá-los a práticas de proteção, deixarão expostos todos os dados sensíveis da companhia (WESTCON, 2016).

Para evitar tais problemas, como perda de informações, algumas dicas de segurança são essenciais na visão de Westcon (2016).

I) Possuir um antivírus no dispositivo como ficam conectados a maior parte do tempo, a exposição a vírus é grande, por isso, um antivírus eficiente garante a proteção do dispositivo e, ainda, pode ajudar em seu desempenho, como possuir softwares de bloqueio de pop-ups, programa antirroubo e bloqueio contra spam.

II) Alteração de senhas periodicamente usar a mesma senha em todos os dispositivos por muito tempo pode ser arriscado. O ideal é modificá-la a cada três meses e usar uma combinação de números e letras.

III) Cuidado ao abrir e-mails é muito comum utilizar smartphones para checar a caixa de e-mails, porém, muitos vírus podem ser anexados a eles. Por isso, deve-se ter cuidado com remetentes desconhecidos ou títulos estranhos.

IV) Uso de redes wi-fi abertas pontos de conexões públicas sempre trazem riscos. Realizar compras online ou outras operações que utilizem dados pessoais deve ser evitado.

V) Modificação do sistema evite procedimentos de desbloqueios não oficiais, pois essas alterações podem incluir vírus ou programas que permitam o controle remoto do aparelho.

VI) Navegação segura há sites com vírus que são preparados para infectar especialmente dispositivos móveis. Durante o acesso, é possível identificar qual é o tipo de aparelho do visitante e tentar ataques específicos para cada tipo de equipamento.

VII) Backup na nuvem realizar cópias de segurança é uma tarefa importante para o caso de roubos ou perdas de dados não salvos, a falta de políticas de segurança móvel deixa os dados sensíveis ainda mais vulneráveis, por isso, deve ser criada e conter regras de autenticação e restrições e exigir o uso de senhas.

A política de uso de aparelhos móveis deve ser parte do processo de integração de corporações, deve ser lida e assinada antes de novos funcionários receberem aparelhos da empresa ou acessarem os recursos da companhia com seus dispositivos pessoais.

Quando o dispositivo é infectado, o usuário se torna exposto ao roubo de informações, vazamento de imagens, números da lista de contato, dados ao sistema operacional e até no hardware.

Muitas vezes esses ataques ocorrem de forma sutil, porém há alguns problemas que podem detectar que o aparelho foi infectado, como a bateria acabar mais rápido do que o normal, o dispositivo tentar se conectar sozinho aos outros via Bluetooth (WESTCON, 2016).

2.4 BYOD

Hoje em dia é quase impossível viver sem um aparelho smartphone ou um tablet, tanto que em muitas empresas está surgindo um fenômeno que não terá mais volta o BYOD (Bring Your Own Device)**,** que é o uso de aparelhos de funcionários na empresa.

Sendo que esta atitude pode facilitar e muito o trabalho desta geração, mas que ao mesmo tempo pode ser um grande desafio para as empresas, que devem criar um equilíbrio entre a segurança da empresa e a possibilidade de se trabalhar com o seu próprio aparelho (MARTINS, 2014).

Segurança da informação infraestrutura avançada e analytics, Francisco Camargo (2013), fenômenos como o BYOD demandam um novo conceito de proteção, agora voltado ao usuário, o que requer mais flexibilidade, redução de custos e mais segurança aos colaboradores.

Entendemos que este conceito de Proteção ao Usuário inova na medida em que foca nos sérios desafios que surgem com a utilização de dispositivos diversos, que vão e vêm de outros ambientes para a empresa.

Mudando as necessidades de proteção e aumentando a complexidade das ameaças, o que exige tratamento constante por parte da área de segurança, o conceito também agrega valor às organizações em termos de redução de custos, flexibilidade de gerenciamento e eficácia na proteção dos seus usuários", avalia o CEO da CLM latino-americano focado em segurança da informação infraestrutura avançada e analytics (CAMARGO, 2013).

Ainda segundo Camargo (2013), é adotado em algumas empresas onde os gestores deixam os funcionários com total liberdade para trabalhar com seus proprios dispositivos integrando dados da empresa com acesso fácil em qualquer lugar.

Permitindo realizar tarefas sem a necessidade de estar presente no local de trabalho isso exige um planejamento por parte da empresa oferecendo suporte técnico, documentação de políticas de acesso ao conteudo, a empresa tem uma redução de custos pois não precisa fazer investimentos com hardware, dados e voz.

Os funcionários podem ter a liberdade de escolher qual dispositivo utilizar no trabalho, com maior produtividade em deselvolver as atividades pois estão familiarizadas com seus dispositivos, enquanto isso, o ambiente BYOD pode ser dinâmico, já que os dispositivos móveis podem mudar com freqüência, novos dispositivos podem se juntar ao ambiente BYOD.

E alguns antigos e não utilizados precisam ser renovados no local de trabalho as versões de hardware e software dos dispositivos são estáveis em um determinado período, de modo que as atualizações de dispositivos e componentes sejam mais faceis de gerenciar.

É impossivel bloquear esse conceito de alguma forma ou outra os usuários descobrem uma maneira de acessar os dados da empresa, isso traz uma grande preocupação com a exposição indevida desses dados, algumas dúvidas surgem relacionadas as estratégias que a corporação deve adotar:

- Definir quais aplicações serão permitidas pela política BYOD da empresa;
- Definir quem vai pagar conta relacionada as taxas de utilização e compra de dispositivos novos;

- Definir quem fornecerá o suporte;
- Definir a utilização pessoal razoavél sem ultrapassar o limite;

De acordo com pesquisa DELL/KACE (2011) Mais de 1.500 CIOs de diferentes empresas. Destes, 48% responderam que não autorizam a prática de BYOD por entenderem que apenas confiar ou simplesmente proibir não seja a alternativa mais eficaz para a mitigação dos riscos.

Porém, concordam que se faz necessárias mudanças na cultura, infraestrutura, suporte, custos, políticas, segurança e governança dentro das corporações para a implantação desta prática.

Temos o fenômeno da consumerização que trouxe uma nova forma de conciliar diversas tarefas em um único gadget, desde acesso à internet, e-mails, e ferramentas Office com o intuito de aumentar a flexibilidade no trabalho diversas práticas, como a do Bring your own technology (BYOT); Bring your own phone (BYOP); Bring your own PC (BYOPC), e o Bring your own device - BYOD (DELL, 2011).

2.5 RISCOS TECNOLÓGICOS

De acordo com Marco Aurélio Maia (2013), poucos usuários de smartphones e tablets possuem antivírus, tornando estes dispositivos alvos fáceis para vírus e outros worms.

Além da infecção por vírus, a própria natureza “móvel” e a fragilidade do processo de autenticação e controle de acesso da grande maioria dos modelos disponíveis no mercado podem facilitar o acesso indevido ou o roubo das informações armazenadas.

Outra questão que atormenta os dirigentes de uma empresa na era BYOD é como minimizar riscos diante da demissão de um colaborador. Ainda de acordo com Marco Aurélio Maia (2013, pg.15) algumas dicas úteis são:

Políticas de BYOD

I) As normas dessa política devem ser apresentadas de forma clara e incluir todos os detalhes em relação à permissão e proibição do uso de recursos pessoais.

II) Defina um Acordo de Confidencialidade e não Divulgação. Este tipo de iniciativa restringe legalmente a possibilidade de saída do capital intelectual da empresa.

III) Estabeleça através da configuração, quem deve acessar os arquivos e serviços de TI da empresa. Monitore os acessos sobre essas informações.

IV) Verifique regularmente a segurança de todos os dispositivos que tenham permissão para acessar as redes da empresa.

Esta regra deve estar clara no contrato assinado pelo colaborador, que deve estar ciente de que a empresa tem esta permissão.

Um relatório elaborado pela Juniper Research (2014), *Mobile Security Strategies*: *Threats*, *Solutions and Market Forecasts*, estima que o número de dispositivos de propriedade de funcionários sendo implantados em empresas chegará a 350 milhões até 2014.

Diante do cenário atual e da perspectiva para os próximos anos, deve ficar mais clara a noção de que estabelecer regras, responsabilidades, direitas e deveres são os primeiros passos para adotar o BYOD com segurança nas organizações.

Ainda de acordo pela empresa Juniper Research (2014), O BYOD é uma realidade crescente nas organizações. É fundamental compreender que, essa não é uma questão que deva ser tratada exclusivamente pela área de TI, apesar dos aspectos tecnológicos.

A interseção com o os departamentos Jurídico e de Recursos Humanos é grande e o trabalho colaborativo entre as áreas é fundamental para se estabelecer uma política sólida e consistente de BYOD.

2.6 DESAFIOS DE SEGURANÇA DAS REDES 4G

De acorde com Mendes (2016), as redes que fornecem serviços de mobilidade evoluíram rapidamente, indo muito além de seu propósito original de prover serviços móveis de voz 4G/LTE (*Long Term Evolution*).

Que são baseadas totalmente em IP, é possível suportar transmissão de dados em altas velocidades, da ordem de Mbps, além dos serviços tradicionais de voz, essa estrutura é fundamental na construção de novos modelos de negócios

baseados em serviços móveis, como mobile banking, Internet das coisas (com aplicações em serviços médicos, vigilância doméstica e telemetria, por exemplo).

Computação em nuvem, distribuição de conteúdo em vídeo e provedores de aplicações e aplicativos, mas junto com essa tecnologia chegam também as questões de segurança, que ganham grande relevância sobre as redes LTE/4G (por serem baseadas em protocolo IP).

Em decorrência disso, novas ameaças a uma operadora de serviços móveis podem ser identificadas como violação de confidencialidade (como tentativas maliciosas de espionagem de tráfego de usuário), violação de integridade (manipulação de dados da operadora de forma não autorizada, incluindo tráfego de controle e sinalização), redução de disponibilidade (abuso da infraestrutura de rede da operadora, exaurindo seus recursos) e fraude (acesso a serviços originalmente não autorizados).

Entre outras, as ameaças são pontencializadas à medida que os assinantes terão em suas mãos smartphone cada vez mais potentes, pelo fato de a arquitetura 4G considerar o uso de redes externas (como WLANs não controladas por operadoras) como novas formas de acesso e de ameaças avançadas (malwares) se propagarem cada vez mais rápido em redes IP, do ponto de vista quantitativo.

O cenário ganha mais relevância no mercado brasileiro onde, segundo a Telebrasil, o número de acessos de banda larga móvel é aproximadamente oito vezes maior do que o acesso fixo, e segundo a IDC, até 2017, 87% dos dispositivos conectados à internet serão smartphones ou tablets, neste cenário, as operadoras devem se preparar para desafios por meio da construção de uma arquitetura de segurança robusta e flexível.

E que, ao mesmo tempo, garanta pelo menos a interoperabilidade com sistemas legados (redes 2G/3G/3.5G), uma transição suave para IPv6 e o suporte à virtualização de sua infraestrutura, lembrando que, como em qualquer outra tecnologia, o uso de segurança não pode afetar o desempenho do sistema, muito menos prejudicar a experiência do usuário. Os *Next Generation Firewalls* (NGFw), com arquiteturas de hardware e de software especializadas, juntamente com plataformas de gerenciamento associadas, estão preparados para estes desafios, ao mesmo tempo que devem ser capazes de proteger recursos críticos na rede

contra-ataques cibernéticos e processar o crescente volume de tráfego demandado por seus usuários.

Ainda de acordo com Mendes (2016), os NGFw também podem suportar a oferta de novos serviços e proporcionar um aumento de receita das operadoras. Pacotes de valor adicionado, como filtragem de conteúdo web, filtros de malware, serviços antispam e prevenção de perda de dados, entre outros, podem ser oferecidos a usuários individuais, grupos de usuários (como clientes corporativos possuidores de smartphones) ou ainda específicos para dispositivos como sensores usados em tecnologias de Internet das coisas.

2.7 ASPECTOS TRABALHISTAS

No Brasil, os trabalhadores são amparados pela Consolidação das Leis Trabalhistas (CLT) que foi criada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, e sancionada pelo presidente Getúlio Vargas, durante o período do Estado Novo.

Já nos dias de hoje, em um contexto muito distinto, os tribunais trabalhistas e a doutrina exerceram um papel de suma importância, na medida em que buscam uma interpretação evolutiva e atual que possa incorporar as novas práticas.

A exemplo é a atualização da Lei 12.551 de 15.12.2011 (publicada no D.O.U de 16.12.2011), já em vigor desde sua publicação, que deu ao artigo 6º da CLT a seguinte redação:

Segundo Balbino (2011) não se distingue entre o trabalho realizado no estabelecimento do empregador, o executado no domicílio do empregado e o realizado a distância, desde que estejam caracterizados os pressupostos da relação de emprego. Parágrafo único: Os meios telemáticos e informatizados de comando, controle e supervisão se equiparam, para fins de subordinação jurídica, aos meios pessoais e diretos de comando, controle e supervisão do trabalho alheio.

2.8 TIPOS CRIPTOGRAFIA

Segundo Desiderá (2016), A criptografia, considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código, é um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos

associados ao uso da Internet, à primeira vista ela até pode parecer complicada, mas para usufruir dos benefícios que proporciona não precisar estudá-la profundamente e nem ser nenhum matemático experiente.

Atualmente, a criptografia já está integrada ou pode ser facilmente adicionada à grande maioria dos sistemas operacionais e aplicativos e para usá-la, muitas vezes, basta a realização de algumas configurações ou cliques de mouse (DESIDERÁ, 2016, pg.50).

Por meio do uso da criptografia pode-se:

- Proteção como o seu arquivo de senhas e a sua declaração de Imposto de Renda;
- Criar uma área (partição) específica no seu computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas;
- Proteger seus *backups* contra acesso indevido, principalmente aqueles enviados para áreas de armazenamento externo de mídias;
- Proteger as comunicações realizadas pela Internet, como os *e-mails* enviados/recebidos e as transações bancárias e comerciais realizadas.

De acordo com o tipo de chave usada, os métodos criptográficos podem ser subdivididos em duas grandes categorias: criptografia de chave simétrica e criptografia de chaves assimétricas.

Criptografia de chave simétrica**:** também chamada de criptografia de chave secreta ou única, utiliza uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados.

Casos nos quais a informação é codificada e decodificada por uma mesma pessoa não há necessidade de compartilhamento da chave secreta. Entretanto, quando estas operações envolvem pessoas ou equipamentos diferentes, é necessário que a chave secreta seja previamente combinada por meio de um canal de comunicação seguro (para não comprometer a confidencialidade da chave). Exemplos de métodos criptográficos que usam chave simétrica são: AES, Blowfish, RC4, 3DES e IDEA.

Criptografia de chave pública, utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono.

Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. Qual chave usar para codificar depende da proteção que se deseja, se confidencialidade ou autenticação, integridade e não-repúdio.

A chave privada pode ser armazenada de diferentes maneiras, como um arquivo no computador, um *smartcard* ou um *token*. Exemplos de métodos criptográficos que usam chaves assimétricas são: RSA, DSA, ECC e Diffie-Hellman.

Ainda Desiderá (2016), diz que chave simétrica, quando comparada com a de chaves assimétricas, é a mais indicada para garantir a confidencialidade de grandes volumes de dados, pois seu processamento é mais rápido. Todavia, quando usada para o compartilhamento de informações, se torna complexa e pouco escalável, em virtude da:

- Necessidade de um canal de comunicação seguro para promover o compartilhamento da chave secreta entre as partes (o que na Internet pode ser bastante complicado) e;
- Dificuldade de gerenciamento de grandes quantidades de chaves (imagine quantas chaves secretas seriam necessárias para você se comunicar com todos os seus amigos).

A criptografia de chaves assimétricas, apesar de possuir um processamento mais lento que a de chave simétrica, resolve estes problemas visto que facilita o gerenciamento (pois não requer que se mantenha uma chave secreta com cada um que desejar se comunicar) e dispensa a necessidade de um canal de comunicação seguro para o compartilhamento de chaves (DESIDERÁ, 2016).

Para aproveitar as vantagens de cada um destes métodos, o ideal é o uso combinado de ambos, onde a criptografia de chave simétrica é usada para a codificação da informação e a criptografia de chaves assimétricas.

É utilizada para o compartilhamento da chave secreta (neste caso, também chamada de chave de sessão). Este uso combinado é o que é utilizado

pelos navegadores *Web* e programas leitores de *e-mails*. Exemplos de uso deste método combinado são: SSL, PGP e S/MIME.

Desiderá (2016), diz que uma função de resumo é um método criptográfico que, quando aplicado sobre uma informação, independente do tamanho que ela tenha, gera um resultado único e de tamanho fixo, chamado *hash.*

- Verificar a integridade de um arquivo armazenado em seu computador ou em seus *backups*;
- Verificar a integridade de um arquivo obtido da Internet (alguns *sites*, além do arquivo em si, também disponibilizam o *hash* correspondente, para que você possa verificar se o arquivo foi corretamente transmitido e gravado);
- Gerar assinaturas digitais.

Para verificar a integridade de um arquivo, por exemplo, você pode calcular o *hash* dele e, quando julgar necessário, gerar novamente este valor. Se os dois *hashes* forem iguais então você pode concluir que o arquivo não foi alterado.

Caso contrário, este pode ser um forte indício de que o arquivo esteja corrompido ou que foi modificado. Exemplos de métodos de *hash* são: SHA-1, SHA-256 e MD5.

A assinatura digital permite comprovar a autenticidade e a integridade de uma informação, ou seja, que ela foi realmente gerada por quem diz ter feito isto e que ela não foi alterada.

A assinatura digital baseia-se no fato de que apenas o dono conhece a chave privada e que, se ela foi usada para codificar uma informação, então apenas seu dono poderia ter feito isto, a verificação da assinatura é feita com o uso da chave pública, pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo.

De acordo com Desiderá (2016), para contornar a baixa eficiência característica da criptografia de chaves assimétricas, a codificação é feita sobre o *hash* e não sobre o conteúdo em si, pois é mais rápido codificar o *hash* (que possui tamanho fixo e reduzido) do que a informação toda, como dito anteriormente, a chave púbica pode ser livremente divulgada. Entretanto, se não houver como comprovar a quem ela pertence, pode ocorrer de você se comunicar, de forma cifrada, diretamente com um impostor.

Um impostor pode criar uma chave pública falsa para um amigo seu e enviá-la para você ou disponibilizá-la em um repositório. Ao usá-la para codificar uma informação para o seu amigo, você estará, na verdade, codificando-a para o impostor, que possui a chave privada correspondente e conseguirá decodificar, uma das formas de impedir que isto ocorra é pelo uso de certificados digitais.

O certificado digital é um registro eletrônico composto por um conjunto de dados que distingue uma entidade e associa a ela uma chave pública. Ele pode ser emitido para pessoas, empresas, equipamentos ou serviços na rede (por exemplo, um *site Web*) e pode ser homologado para diferentes usos, como confidencialidade e assinatura digital.

Um certificado digital pode ser comparado a um documento de identidade, por exemplo, o seu passaporte, no qual constam os seus dados pessoais e a identificação de quem o emitiu. No caso do passaporte, a entidade responsável pela emissão e pela veracidade dos dados é a Polícia Federal, no caso do certificado digital esta entidade é uma Autoridade Certificadora (AC).

Uma AC emissora é também responsável por publicar informações sobre certificados que não são mais confiáveis. Sempre que a AC descobre ou é informada que um certificado não é mais confiável, ela o inclui em uma "lista negra", chamada de "Lista de Certificados Revogados" (LCR) para que os usuários possam tomar conhecimento. A LCR é um arquivo eletrônico publicado periodicamente pela AC, contendo o número de série dos certificados que não são mais válidos.

Os certificados digitais são apresentados nos navegadores *Web*. Note que, embora os campos apresentados sejam padronizados, a representação gráfica pode variar entre diferentes navegadores e sistemas operacionais. De forma geral, os dados básicos que compõem um certificado digital são:

- Versão e número de série do certificado;
- Dados que identificam a AC que emitiu o certificado;
- Dados que identificam o dono do certificado (para quem ele foi emitido);
- Chave pública do dono do certificado;
- Validade do certificado (quando foi emitido e até quando é válido);

- Assinatura digital da AC emissora e dados para verificação da assinatura.

2.9 PROTEÇÃO DOS DADOS

- Utilizar criptografia sempre que, ao enviar uma mensagem, quiser assegurar-se que somente o destinatário possa lê-la;
- Utilizar assinaturas digitais sempre que, ao enviar uma mensagem, quiser assegurar ao destinatário que foi você quem a enviou e que o conteúdo não foi alterado;
- Só enviar dados sensíveis após certificar-se de que está usando uma conexão segura.
- Utilizar criptografia para conexão entre seu leitor de *e-mails* e os servidores de *e-mail* do seu provedor;
- Cifrar o disco do seu computador e dispositivos removíveis, como disco externo e *pen-drive*. Desta forma, em caso de perda ou furto do equipamento, seus dados não poderão ser indevidamente acessados;
- Verificar o *hash*, quando possível, dos arquivos obtidos pela Internet isto permite que você detecte arquivos corrompidos ou que foram indevidamente alterados durante a transmissão (DESIDERÁ, 2016).

2.10 CUIDADOS COM AS CHAVES E CERTIFICADOS

- Utilizar chaves de tamanho adequado. Quanto maior a chave, mais resistente ela será a ataques de força bruta.
- Não utilizar chaves secretas óbvias.
- Certificar-se de não estar sendo observado ao digitar suas chaves e senhas de proteção.
- Utilizar canais de comunicação seguros quando compartilhar chaves secretas.
- Armazenar suas chaves privadas com algum mecanismo de proteção, como por exemplo senha, para evitar que outra pessoa faça uso indevido delas.

- Preservar suas chaves. Procure fazer *backups* e mantenha-os em local seguro (se você perder uma chave secreta ou privada, não poderá decifrar as mensagens que dependiam de tais chaves).
- Ter muito cuidado ao armazenar e utilizar as chaves em computadores potencialmente infectados ou comprometidos, como em *LAN houses*, *cybercafes*, *stands* de eventos, etc.
- Se suspeitar que outra pessoa teve acesso à sua chave privada (por exemplo, porque perdeu o dispositivo em que ela estava armazenada ou porque alguém acessou indevidamente o computador onde ela estava guardada), solicite imediatamente a revogação do certificado junto à AC emissora.

2.11 CUIDADOS AO ACEITAR UM CERTIFICADO DIGITAL

- Manter o sistema operacional e navegadores *Web* atualizados (além disto contribuir para a segurança geral do seu computador, também serve para manter as cadeias de certificados sempre atualizadas);
- Manter o computador com a data correta. Além de outros benefícios, isto impede que certificados válidos sejam considerados não confiáveis e, de forma contrária, que certificados não confiáveis sejam considerados válidos.
- Ao acessar um *site Web*, observe os símbolos indicativos de conexão segura e leia com atenção eventuais alertas exibidos pelo navegador.
- o navegador não reconheça o certificado como confiável, apenas prossiga com a navegação se tiver certeza da idoneidade da instituição e da integridade do certificado, pois, do contrário, poderá estar aceitando um certificado falso, criado especificamente para cometer frauds (DESIDERÁ, 2016).

3 PROCEDIMENTOS METODOLÓGICOS

Para elaboração da fundamentação teórica foi feita uma pesquisa bibliográfica e uma pesquisa documental, relatando as definições e os demais aspectos que se referem a DFC.

Segundo Marconi, Lakatos (1990, pg. 66) “a pesquisa bibliográfica ou de fontes secundarias, abrange toda bibliografia já tornada pública em relação ao tema de estudo, desde publicações avulsas, boletins, jornais, revistas, livros, pesquisas, monografias, material cartográfico etc”.

Segundo os mesmos autores, a característica da pesquisa documental é “que a fonte de coleta de dados está restrita a documentos, escritos ou não, constituindo o que se denomina fontes primarias”, onde a empresa disponibiliza os relatórios contábeis e demais dados que se julguem necessários.

3.1 FONTES DE PESQUISA

Foi realizada uma pesquisa bibliográfica em sites, como por exemplo, *ComputerWorld, Cartilha, Imasters*, para identificar as políticas de uso e segurança sobre aplicação BYOD.

Identificaram-se, também, nestes materiais as principais tecnologias para manter a segurança dos dados corporativos, tais como *Network Access Control* e *Mobile Application Management* e os cuidados com a utilização de dispositivos móveis, os desafios de segurança que a empresa precisa ter ao implantar a modalidade como por exemplo as leis trabalhistas.

A literatura, indica que uma política de segurança bem implantada, o risco de perda dos dados corporativos são mínimos.

3.2 CLASSIFICAÇÃO DA PESQUISA

A Pesquisa Científica visa a conhecer cientificamente um ou mais aspectos de determinado assunto. Para tanto, deve ser sistemática, metódica e crítica. O produto da pesquisa científica deve contribuir para o avanço do conhecimento humano. Na vida acadêmica, a pesquisa é um exercício que permite

despertar o espírito de investigação diante dos trabalhos e problemas sugeridos ou propostos pelos professores e orientadores.

3.3 MÉTODOS DE ANÁLISE DOS RESULTADOS

O método de pesquisa exploratória teve o objetivo de trazer um maior entendimento sobre o fenômeno BYOD.

4 RESULTADOS E ANÁLISES DE DADOS

Neste capítulo são apresentadas as ferramentas de BYOD que ajudam na proteção e confidenciabilade dos dados corporativos.

4.1 NETWORK ACCESS CONTROL - NAC

Network Access Control é uma tecnologia que mantem a proteção contra-ataques na rede, ao longo das últimas décadas, as empresas e os administradores de rede estavam preocupados apenas em conseguir colaboradores e parceiros de negócios, mas agora com o avanço das redes e a tecnologia, o foco mudou.

O interesse é não permitir acessos não-autorizados na rede e bloquear conteúdo que não tenha a ver com os negócios da empresa, o nac se tornou uma ferramenta fundamental contra-ataques, ela ajuda a empresa a reforçar a segurança das suas políticas em qualquer aparelho conectado na rede ou tentando a conexão (FALSARELLA, 2010).

4.2 TIPOS DE NAC E FUNCIONALIDADE

As tecnologias NAC são oferecidas por vários fornecedores diferentes e apresenta uma ampla variedade de tipos. Algumas das mais utilizadas pelos vendors NAC são:

- **Agent-Based**: O agente se comunica com o servidor, e autentica uma rede conectada servidor NAC ou aparelho. A abordagem é simples, mas é relativamente rígida e requer um software especial para ser instalada e aplicada em dispositivos de usuário final.
- **Agentless**: Com a opção do NAC sem agente, não há necessidade de instalar agentes especiais na área de trabalho individual e computadores portáteis e dispositivos de usuário final de outro. Em vez disso, um agente é

armazenado em um diretório temporário. Evitar agentes torna mais fácil a implantação e simplifica as operações NAC.

- **Inline**: Um NAC inline tem todo o tráfego que passa através dele. O NAC funciona como um firewall de camada de redes de acesso, reforçando as políticas de segurança. Embora conveniente, esta abordagem pode criar gargalos throughput em redes maiores. Essa configuração também pode aumentar os custos ao longo do tempo, uma vez que mais dispositivos embutidos devem ser acrescentados ao tráfego crescente.
- **Out-of-Band**: uma alternativa para uma NAC inline é usar um out-of-band. Out-of-band utilizam as capacidades de execução de infra-estrutura da rede. Com esta técnica, os agentes são normalmente distribuídos como clientes que repassam os dados para um console central, que pode comandar a aplicar a política. A abordagem é mais complexa, mas exerce um impacto mínimo sobre o desempenho da rede.

Todas estas tecnologias ajudam com a segurança de falhas e perdadas de informações

NAC são produzidos por diversas empresas, elas desenvolvem as funcionalidades para segurança dos dispositivos incluindo os líderes de mercado tais como:

- Cisco Systems Inc.
- ConSentry Networks
- InfoExpress Motores de Identidade Inc.
- Vernier Networks Inc.

4.3 ARQUITERURA NAC

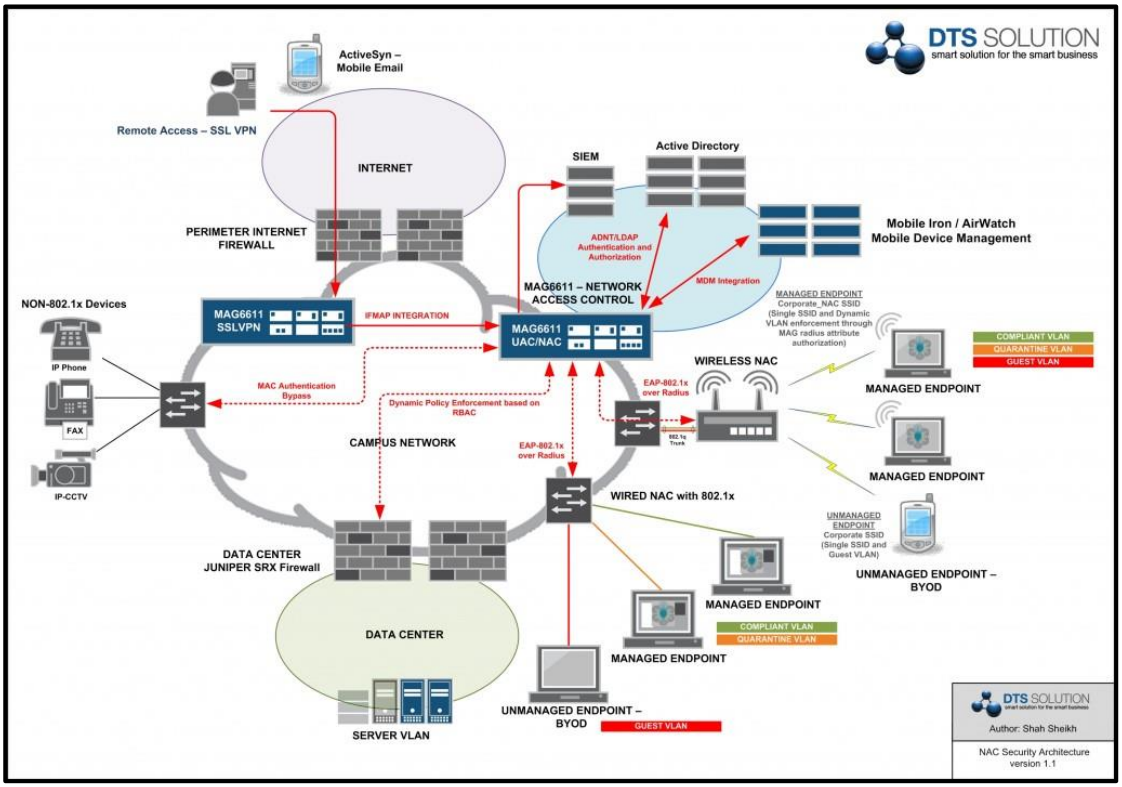
Projetar e implantar a solução NAC direita para atender aos seus requisitos de conformidade é primordial para garantir que um modelo de controle de acesso consistente seja aplicado aos diferentes perfis de usuários.

Ao fornecer acesso de rede dinâmico com base em perfis de usuários e privilégios é a chave para uma implantação bem-sucedida.

A compreensão dos pontos-chaves na integração NAC com autenticação, serviços de auto-remediação, atribuição de VLAN dinâmica com base na conformidade e reputação do ponto final e na concepção da solução certa.

A Figura 1 apresenta um cenário NAC com todas as funcionalidades de proteção.

Figura 1 – Arquitetura NAC



Fonte: dts solution (2017).

Segundo Falsarella (2010) um NAC garante que todos os terminais (computadores) da rede fiquem conforme as regras de segurança da empresa, protege os recursos de infra-estrutura, assegurando a produtividade dos funcionários, ela também bloqueia os recursos gerenciados e não gerenciados enquanto permite acesso seguro ao visitante.

Falsarella (2010), também reforça as políticas de acesso à base de identidades de usuários autenticados na rede, no mercado existe a opção open source de *network access control* oferecem interfaces de usuários melhoradas e o suporte avançado disponíveis nas ferramentas pagas, oferecem alguma integração limitada com outros produtos.

Mas nenhum deles possui a ampla gama de suporte à terceiros disponíveis em um produto comercial, os produtos NAC garantem que computadores e laptops conectados à rede estejam em conformidade com as

políticas da organização e que medidas de quarentena e isolamento sejam tomadas.

Para os dispositivos comprometidos até que eles estejam limpos e reparados. O NAC não faz somente a verificação dos computadores usados pelos empregados, mas também verifica a o estado de cada equipamento (FALSARELLA, 2010).

A separação de redes para visitantes e funcionários ajuda no controle de tipo de acessos de cada um.

4.4 MOBILE DEVICE MANAGEMENT - MDM

Segundo Ferril (2017), um dispositivo móvel corporativo perdido representa uma ameaça para empresa a ferramenta MDM fornece a capacidade de localizar, bloquear e potencialmente limpar dispositivos perdidos tem a capacidade de devolver o telefone ao estado em que estava antes de se iniciar no gerenciamento de dispositivos móveis.

Isso inclui a remoção de configurações, como senhas Wi-Fi, configurações e documentos protegidos, esse recurso pode ser ajustado para funcionários que viajam e, em muitos casos, também pode ter tempo restrito, configurar dispositivos para bloquear com um número de identificação pessoal (PIN).

É apenas uma das muitas políticas que podem ser definidas como obrigatórias, O que significa que, mesmo que um dispositivo seja de propriedade do empregado em um cenário BYOD, uma vez que esteja registrado, ele exigirá um PIN para abrir se o usuário se definiu dessa forma ou não.

Outras políticas para restringir o comportamento ou bloquear aplicativos específicos também são comuns, mas o conflito entre dispositivos corporativos e de propriedade pessoal nem sempre é tão claro, ter a capacidade de restringir a reunião de localização e outros dados confidenciais de um dispositivo de propriedade pessoal.

Ajudam a manter os funcionários felizes, permitindo que eles usem seus próprios dispositivos para o trabalho da empresa, os gerentes de TI precisam ter cuidado e procurar a capacidade de segmentar o trabalho e os aplicativos e dados

pessoais tanto quanto possível, gerenciamento remoto ao dispositivo com consentimento do funcionário (FERRIL, 2017).

Com a funcionalidade do *Mobile Device Management* ajuda na proteção dos dados referente a perda de informações, segurança anti roubo e perda do dispositivo.

I) Gerencie grupos de dispositivos dividindo hierarquicamente até 5 camadas e também delegação de autoridade disponível.

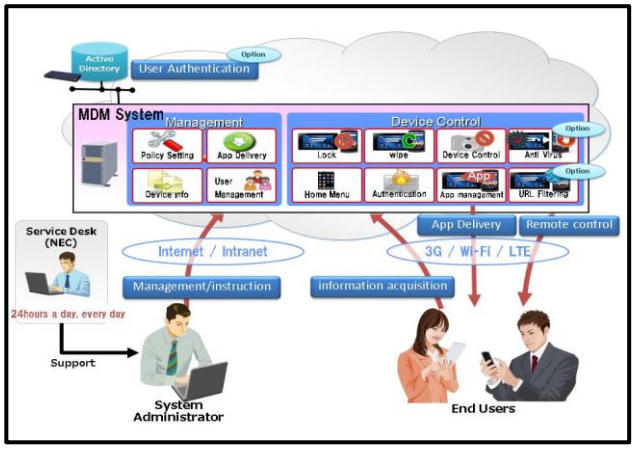
II) Conclua a configuração do dispositivo coletivamente importando arquivos CSV.

III) Confirme a situação de reflexão do perfil do terminal graficamente com um portal de gerenciamento.

IV) Entregue uma aplicação empresarial a todos os dispositivos em um grupo de dispositivos simultaneamente.

A Figura 2 mostra um sistema projetado para grande escala:

Figura 2 - Mobile Device Management (MDM)



Fonte: nec (2016).

Políticas de segurança com autenticação no servidor mostrando relatórios de acessos de tudo o que é feito no dispositivo.

4.5 BENEFÍCIOS COM A IMPLANTAÇÃO MOBILE DEVICE MANAGEMENT

- Gerenciamento da mobilidade
- Segurança com os dados
- Produtividade

- Políticas de utilização
- Redução de custos

4.6 MOBILE APPLICATION MANAGEMENT - MAM

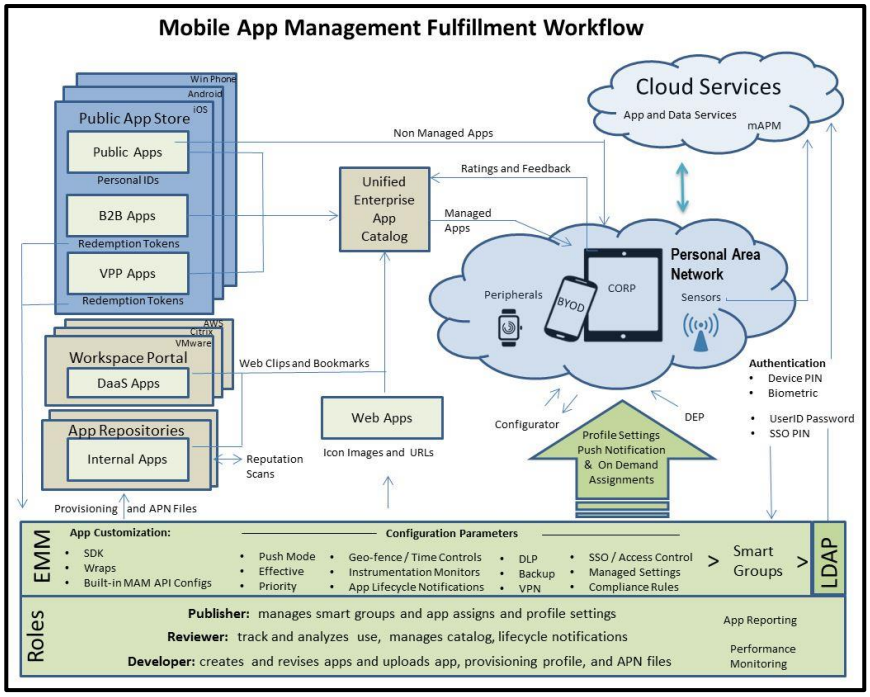
Segundo Madden (2016), *Mobile Application Management* procura aplicar controles EMM a aplicativos individuais ou grupos de aplicativos, em vez de todo o dispositivo, essas tarefas incluem:

- Criptografia de dados do aplicativo.
- Conectividade de rede segura (por aplicativo ou VPN).
- Configurações em aplicativos (endereços de servidor, nomes de usuário).
- Autenticação e SSO para recursos backend acessados pelo aplicativo.
- Aplicar uma senha ou desafio de segurança para abrir aplicativos corporativos. (Isso pode ser o mesmo que o processo de autenticação ou simplesmente um código de acesso local).

Existem muitos componentes e funções convergentes que precisam ser considerados ao puxar uma estrutura abrangente de gerenciamento de aplicativos móveis de ponta a ponta.

A Fígura 3 identifica o que precisa ser coberto na carta de cumprimento de gerenciamento de aplicativos:

Figura 3 – Workflow de uma aplicação MAM



Fonte: unisys (2015).

A Figura 3 mostrando todo procedimento para segurança dos aplicativos no dispositivo móvel.

Observa-se que o compartilhamento de dados seguro entre aplicativos empresariais e mantenha os dados corporativos fora de aplicativos pessoais, Existem todos os tipos de formas diretas e indiretas para compartilhar dados, abrir extensões de aplicativos, intenções e repositórios de sistema, como álbuns de fotos ou calendários.

Limpeza remota de dados ou desativação do aplicativo, existe outras tarefas relacionadas, como análises, monitoramento de desempenho e todo o processo do ciclo de vida de criar, assinar, distribuir e atualizar aplicativos, isso também é importante.

Mas eles representam um conjunto diferente de problemas, existem duas formas principais para que todos esses recursos e tarefas de gerenciamento sejam aplicados, os recursos de gerenciamento podem ser criados diretamente nos próprios pacotes de aplicativos, MAM de nível de aplicativo, outro termo que está se tornando comum é MAM autônomo, muitos dispositivos móveis possuem estruturas de gerenciamento integradas que podem diferenciar entre aplicativos empresariais e dados e dados pessoais. Esses quadros dependem da inscrição subjacente do MDM, também é conhecido como a abordagem *"AppConfig*". Aplicativos que vêm

diretamente dos vendedores do EMM e que os recursos do MAM são incorporados, os primeiros exemplos foram os clientes de e-mail, como o Good for Enterprise, os exemplos também podem incluir navegadores, sincronização de arquivos e compartilhar aplicativos.

Editores de documentos, aplicativos de scanner e câmera e mensagens instantâneas, Kit de desenvolvimento de software (SDKs) ou outras bibliotecas com funcionalidades MAM que podem ser incorporadas por desenvolvedores enquanto estão criando aplicativos corporativos, ferramentas de modificação de aplicativos ou aplicativos de aplicativos, eles levam binários de aplicativos pré-compilados existentes e adicionam um wrapper que possui funcionalidade MAM.

Possivelmente incluindo a capacidade de interceptar e redirecionar as chamadas de API do aplicativo. Após o embrulho, os aplicativos são renunciados e redistribuídos, embora houvesse usos mais amplos no passado, hoje a indústria concorda que não pode conter aplicativos de lojas de aplicativos públicos, precisa da permissão do desenvolvedor original ou ISV, muitos fornecedores de EMM têm programas para encorajar ISVs a incorporar seus SDK MAM em seus aplicativos.

Ainda de acordo com Madden (2016), alguns aplicativos orientados para a empresa também possuem recursos próprios do MAM, configurados nos serviços de back-end dos aplicativos, em vez de depender de plataformas EMM ou MAM, os recursos do MAM em aplicativos podem compensar as falhas do dispositivo, reduzir os efeitos da fragmentação do Android e até mesmo permitir que aplicativos sejam executados em dispositivos não confiáveis .

Não é necessário o gerenciamento de dispositivos móveis, o que ajuda a aliviar as preocupações com a privacidade do usuário, o MAM do nível de aplicativo é inerentemente limitado aos aplicativos criados com as técnicas acima em mente, no caso de clientes de e-mail, o desempenho de aplicativos de terceiros pode não ser tão bom quanto os clientes que estão empacotados com sistemas operacionais móveis.

Os frameworks MAM do nível de aplicativo são proprietários de diferentes fornecedores de EMM, isso pode ser um problema para os clientes, porque a escolha da plataforma EMM pode limitar os aplicativos que podem gerenciar (MADDEN, 2016).

Esse tipo de solução coloca obstaculos sobre o dispositivo alertas informa a entrada do dispositivo dentro do ambiente corporativo, ferramentas de

controle remoto são capazes de desligar o dispositivo ou até mesmo apagar todos os dados.

4.7 DESKTOP AS A SERVICE - DAAS

De acordo com Gohring (2014), Os aplicativos empresariais nem sempre estão disponíveis nos dispositivos de escolha dos usuários, Desktop as a Service (DaaS) está se tornando uma maneira de resolver esse problema, DaaS fornece desktops virtualizados da nuvem, os desktops podem ser personalizados para grupos de trabalhadores, em torno de níveis ou funções específicas de trabalho.

Comercialmente disponível por quase uma década, a DaaS foi inicialmente destinada a descarregar tarefas de gerenciamento e espalhar os custos da infra-estrutura de desktop virtual tradicional (VDI), mas DaaS recentemente começou a crescer, de acordo com Scott Ottaway, um analista da 451 Research, o *desktop hosting* é agora um mercado de US $ 2 bilhões para fornecedores de serviços em nuvem.

Também é possível criar uma configuração DaaS em servidores internos, semelhante à criação de uma nuvem privada, muitos fatores aceitação da nuvem, diversidade de dispositivos, mão-de-obra móvel e acesso onipresente à Internet - combinaram-se para tornar a DaaS atrativa para algumas empresas, e há mais fornecedores de marca: em meados de 2012, a Dell comprou a Quest Software, que oferece a DaaS entre outros serviços, desde então, a VMware adquiriu o Desktone, um provedor DaaS, e a Amazon lançou seu serviço de desktop virtual WorkSpaces.

Existem algumas razões pelas quais o conceito vem atraindo interesse renovado, há uma força de trabalho cada vez mais móvel trabalhando em uma gama cada vez maior de dispositivos, e as organizações de TI estão desesperadas para mitigar os afetos dessa complexidade, mas ainda fornecem acesso aos sistemas que as pessoas precisam quando precisam, muitos aplicativos não estão disponíveis no dispositivo de um usuário escolhido, como um iPad.

A grande maioria dos aplicativos empresariais ainda são baseados no Windows, enquanto os aplicativos SaaS podem ajudar os usuários a fazerem algum trabalho em qualquer lugar com qualquer dispositivo, pois eles são acessíveis por navegador.

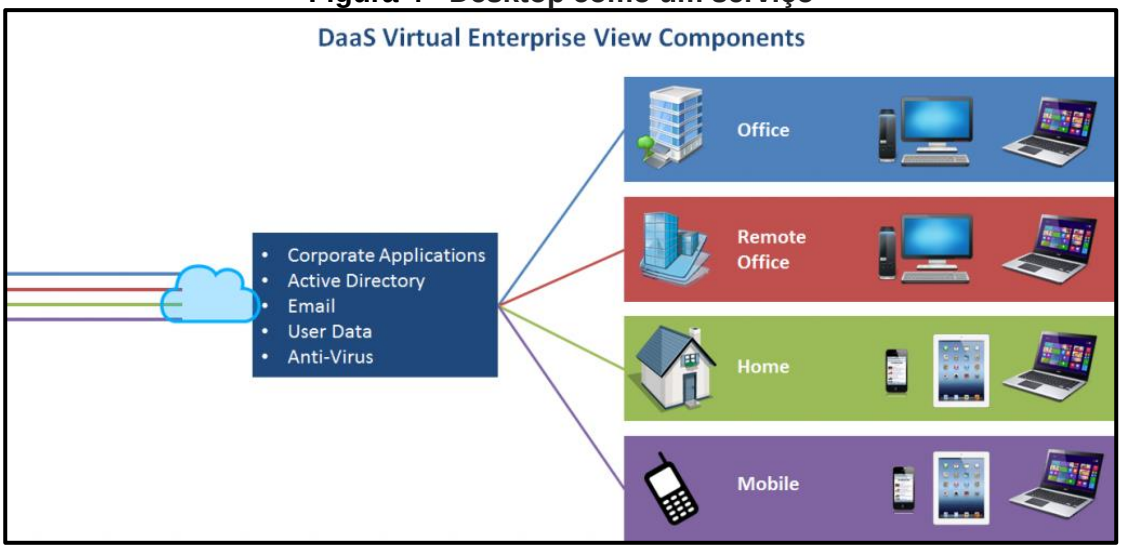
O SaaS não resolve o problema porque muitos aplicativos corporativos ainda não estão disponíveis no formulário SaaS, explica Ottaway. Em contraste, a DaaS oferece uma experiência de desktop Windows (ou Linux), bem como aplicativos compatíveis com o Windows, para dispositivos que incluem iPads, além disso, mais empresas ficam confortáveis com os serviços da nuvem.

Quando DaaS saiu pela primeira vez, as empresas tendem a ser mais cautelosas com o uso da nuvem, além disso, a conectividade melhorou ao longo do tempo, com a DaaS, os usuários precisam de uma conexão com a Internet para acessar seus desktops e aplicativos relacionados, as conexões de internet ficaram mais rápidas e os provedores de tecnologia otimizaram protocolos para trabalhar com conexões menos capazes (GOHRING, 2014).

Experiência de usuário de alta definição em qualquer dispositivo, permitindo um ambiente de trabalho completamente controlado e seguro, além de mobilidade e flexibilidade para usuários finais.

A Fígura 4 identifica acessos Home Office.

Figura 4 - Desktop como um serviço



Fonte: Emerio (2017).

A Fígura 4 mostra as Configurações essenciais para ter acesso home office aos dados corporativos.

4.8 RBAC PERMISSÃO BASEADA EM FUNÇÃO

Uma permissão é um elemento crítico do sistema de controle de acesso baseado em função que impede que todo o sistema entre em colapso no caos, a permissão é como um portão que impede algumas ações e permite que outros.

Ao aprender mais sobre o controle de acesso baseado em função, é essencial para redes e segurança de dados, controle de acesso baseado em função é um método de garantir apenas o pessoal autorizado tenha acesso a recursos sensíveis do sistema.

Sem um sistema como este no lugar, os funcionários de baixo nível pode acessar informações financeiras, relatórios e memorandos confidenciais, o controle de acesso baseado em função em empresas com mais de 500 funcionários, oferece uma maneira simples e rápida de organizar os trabalhadores em camadas, cada camada acima da última tem mais acesso a rede e bancos de dados da empresa.

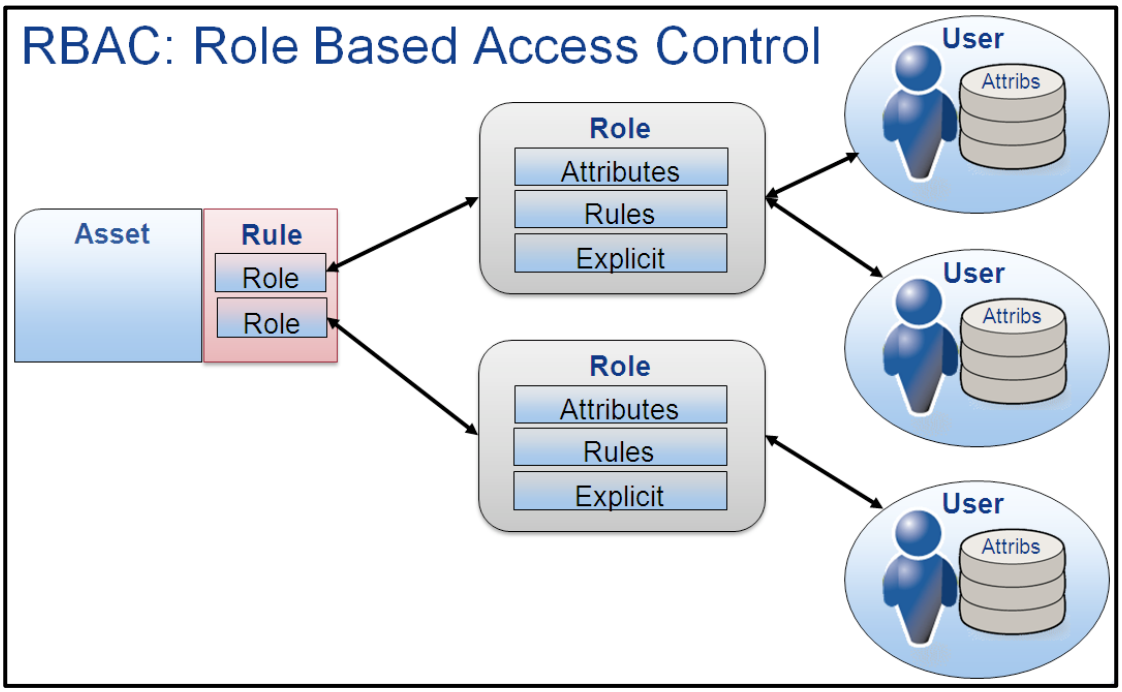
O processo de implementação de controle de acesso baseado em função começa com a atribuição de cada funcionário um papel, podendo criar muitos papéis, mas cada um deve ter um nome único, cada função tem um nível diferente de acesso ao sistema, podendo mudar o papel qualquer funcionário a qualquer momento, deve atribuir ativamente um papel para cada empregado.

Mas uma vez que fizer isso, o sistema irá automaticamente restringir seu movimento em toda a rede da empresa.

A permissão é um ação, ou um conjunto de ações, que alguém atribuído um determinado papel é livre de tomar, quando é criada uma função, é especifica as permissões imediatamente, isto significa que uma vez criado, nunca mais vai ter que atribuir permissões em uma base individual, porque atribuir as pessoas a esse papel, se necessário, isto também significa que pode controlar facilmente os casos de pessoas que tentam acções para as quais eles não têm permissões, qualquer permissão pode ser atribuído a mais de uma função, e que um papel pode ter um número ilimitado de permissões (PT COMPUTADOR, 2015).

O acesso é concedido a um papel. Os indivíduos são associados ao papel e, assim, obtêm acesso aos ativos. A Fígura 5 do RBAC mostram os atributos para permissão de acesso.

Fígura 5 - Função baseada em controle de acesso



Fonte: identitysander (2009).

A Figura 5 mostra da esquerda para a direita no diagrama acima, possui o ativo ao qual o acesso está sendo concedido, depois, existe alguma forma de uma regra que é controlar o acesso a esse bem.

Se o recurso fosse um arquivo, as permissões no sistema de arquivos para esse arquivo seriam a regra, então você tem os papéis.

Os papéis podem ter usuários associados de várias maneiras, os atributos podem determinar o uso do usuário, as regras também podem ser usadas para determinar a associação de papéis.

E um usuário também pode simplesmente ser declarado como tendo uma função explicitamente, por último, tem os usuários e todos os seus atributo

5 CONSIDERAÇÕES FINAIS

Para responder à pergunta de pesquisa, sobre a segurança da implantação de políticas de uso e segurança do conceito BYOD nas empresas observou-se que com uma politica de segurança bem implantada o risco de perda dos dados corporativos são minimos.

O uso dos dispositivos móveis é evidente, cada vez mais frequente e está em alta. Um smartphone, por exemplo, concentra funções interessantes que

vão além da comunicação, com ele é possível fotografar, acessar documentos, localizar lugares no mapa, fazer compras e até controlar uma rotina de exercícios.

A prática de BYOD (Bring Your Own Device) já faz parte da maioria das empresas atualmente e também pode trazer vulnerabilidade aos dados da corporação e dos funcionários, se não houver políticas de segurança e controle de acesso, caso as empresas não possuam sistemas adequados para alertar os funcionários sobre os riscos à segurança e incentivá-los a práticas de proteção, deixarão expostos todos os dados sensíveis da companhia.

Criar uma estratégia dentro do ambiente de trabalho com políticas adequadas e procedimentos tecnológicos, a mobilidade permite que os profissionais executem tarefas e processos em qualquer lugar e a qualquer hora, para minimizar esse risco algumas dicas de segurança é essencial como possuir um antivirus no dispositivo, alterar as senhas periodicamente, acessa a redes wi-fi sem criptografia, backup na nuvem.

O presente trabalho teve por objetivo mostrar os riscos e a segurança envolvida no ambiente corporativo atráves do uso de um dispositivo móvel, a partir de uma análise descritiva dos dados, os dados mostram que foi possível perceber o crescimento BYOD nas empresas, e com uma política de segurança bem implantada de controles podendo reduzir as chances de comprometimento aos dados da empresa.

5.1 LIMITAÇÕES DA PESQUISA E TRABALHOS FUTUROS

Sugere-se para pesquisas futuras que sejam feitas mais análises com as relações trabalhistas e as práticas de Bring your Own Device no ambiente corporativo, pois há vários processos trabalhistas com relação ao BYOD que tratam de perda de dados e uso de dispositivos da empresa.

REFERÊNCIAS

SAGEONE. **byod-o-que-e-e-como-isso-pode-ajudar-na-produtividade-da-sua-empresa. Disponível em** <http://br.sageone.com/2015/03/13/byod-o-que-e-e-como-isso-pode-ajudar-na-produtividade-da-sua-empresa/ >Acesso em 23/01/2017

DAROZ, Kelin. SEBASTIAO DE BARROS, Mauricio. **consumerizacao-nas-organizacoes-praticas-e-gestao-do-byod.** Disponível em <http://direitoeti.com.br/artigos/consumerizacao-nas-organizacoes-praticas-e-gestao-do-byod/ >Acesso em 13/02/2017

FALSARELLA, Douglas. **redes-e-servidores/nac-redes-mais-seguras.** Disponível em <https://imasters.com.br/artigo/17375/redes-e-servidores/nac-redes-mais-seguras/?trace=1519021197&source=single> Acesso em 25/08/2017

FERRILL, Paul. **the-best-mobile-device-management-mdm-software**. Disponível em <https://www.pcmag.com/article/342695/the-best-mobile-device-management-mdm-software> Acesso em 10/09/2017

MADDEN, Brian. **The-complete-guide-to-mobile-application-management-Understanding-different-MAM-techniques.** Disponível em <http://www.brianmadden.com/opinion/The-complete-guide-to-mobile-application-management-Understanding-different-MAM-techniques> Acesso em 01/09/2017

GOHRING, Nancy. **desktop-as-a-service-your-byod-assist**. Disponível em <https://www.computerworld.com/article/2836548/desktop-as-a-service-your-byod-assist.html> Acesso em 18/09/2017

FATEC. **Políticas de segurança da informação para BYOD.** Disponível em <fatec.br/revista_ojs/index.php/RTecFatecAM/article/download/66/77> Acesso em 18/09/2017

PT COMPUTADOR. **O que é um Access Control (RBAC) Permissão baseada em função.** Disponível em **<**http://ptcomputador.com/Networking/network-security/75651.html> Acesso em 10/09/2017

CONVERGENCIA DIGITAL. **Os desafios de segurança das redes 4G/LTE.** Disponível em <http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=42042&sid=15> Acesso em 06/09/2017

DESIDERÁ, Lucimara. **Criptografia.** Disponível em< https://cartilha.cert.br/criptografia/ >Acesso em 19/09/2017

MAIA, Marco. **BYOD. Disponível em<** http://segurancadainformacao.modulo.com.br/o-que-e-byod> Acesso em 19/09/2017