POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO PARA BYOD

Mariana Beltran Cometti
Alexandre Garcia Aguado

RESUMO

Este trabalho apresenta características sobre as políticas de segurança da informação, como podem prevenir, assegurar e auxiliar as organizações. As políticas são essenciais para o bom funcionamento da organização. Além disso, são explicados os conceitos e finalidades de consumerização e do fenômeno BYOD, os quais apresentam a evolução continua e constante e devido a isso devem se enquadrar nas políticas de segurança da informação. Durante o estudo são apresentados outros serviços ligados diretamente ao fenômeno BYOD, que devem ser implantados nas boas práticas das políticas. E através do estudo de caso, se aprofunda a analise de políticas já implantadas para o BYOD e sugestões de políticas que poderão ser implantadas em organizações que utilizam este, porém não tem regras especificas para sua utilização, tornando-a vulnerável a ataques.

Palavras-chave: BYOD; Políticas de Segurança da Informação; Consumerização.

ABSTRACT

This paper presents characteristics of information security policies, how they can prevent, secure and support organizations. Policies are essential to the proper functioning of the organization. Moreover, the concepts are explained and purposes of consumerization and BYOD phenomenon, which present the continuous evolution and constant and because of this must fall on information security policies. During the study are presented ther services directly linked to the BYOD phenomenon that must be deployed on best practice policies. And through the case study, deepens the political analysis already in place for BYOD and policy suggestions that can be implemented in organizations that use this, but does not have specific rules for their use, making it vulnerable to attack.

***Keywords**: BYOD; Policies for Information Security; Consumerization.*

1 INTRODUÇÃO

A tecnologia da informação tem avançado claramente com o decorrer dos anos. Nos anos 60 utilizavam-se mainframes (grandes computadores) para processamento de dados, sua utilização era para fins de controles funcionais, como folha de pagamento, estoque e outros. (REZENDE, 2011)

Passada uma década, nos anos 70, os computadores tinham melhor capacidade de processamento e seu o custo era menor. Com melhor capacidade, eram utilizados para gerenciar estoques e relatórios gerenciais. (SANTOS; FRESCHI, 2013)

Chegando aos anos 80, já havia microcomputadores em mais áreas de trabalho com dados centralizados e utilizados pelos colaboradores nas organizações. Na metade da década, os sistemas utilizados nas organizações eram estratégicos e contribuíam para a competitividade.

O maior avanço veio nos anos 90, década marcada pelo surgimento da *Internet* e o alto desempenho das telecomunicações, mudando a forma de trabalho de todas as organizações e o dia-a-dia das pessoas. Seria o começo da Era da Tecnologia da Informação. (SANTOS; FRESCHI, 2013)

Esse grande impulso ocasionou crescimento para economia e negócios, motivando a competitividade entre as organizações, onde estas se viram obrigadas a enquadrar estratégias nos negócios para acompanhar a evolução tecnológica, para que não se prejudicassem. (SANTOS; FRESCHI, 2013)

Mas o crescimento não pararia ai, as redes sociais começaram a ganhar força, evoluindo constantemente, facilitando a transmissão de informações por meio da *Internet* e trazendo maior acesso as informações para meios corporativos, mas também trazendo problemas de segurança. Tal fato tem impulsionado a exigência de políticas de segurança da informação nas corporações, assunto o qual, será abordado no decorrer deste trabalho.

As organizações também foram aprimorando seus conhecimentos em tecnologia da informação e se adequando as novas fases dessa era. Um computador desktop era utilizado em cada mesa de cada colaborador que a organização julgasse necessário e este, por fim, trabalhava em uma rotina diária, passando cerca de oito horas em frente à tela de um computador, mas isso logo mudaria.

Com a criação de dispositivos móveis, a tecnologia evoluiu mais ainda e a utilização de smartphones não parou mais de crescer. Conforme pesquisa realizada pela Teleco através do estudo IDC *Mobile Phone Tracker* Q4, realizado pela IDC Brasil, o mercado de *smartphones* no Brasil atingiu 54,0 milhões de unidades em 2014, 76,1% do total de celulares comercializados.” (TELECO, 2015, p.1)

Ainda sobre a pesquisa mencionada acima, o Brasil terminou o ano de 2014 com um total de 71,0 milhões de aparelhos comercializados, alcançando a 4ª colocação entre os maiores mercados do mundo, atrás da China, Estados Unidos e Índia. (TELECO, 2015)

Com isso, o fenômeno *Bring Your Own Device* (BYOD), ou seja, a utilização de dispositivos móveis pessoais em corporações para tarefas no trabalho através de *smartphones, notebooks* e *tablets* criado através da evolução da consumerização, trouxe aos negócios das organizações melhor desempenho nos trabalhos diários.

Com a utilização do BYOD, a informação fica disponível ao funcionário em qualquer lugar e a qualquer hora, o que é bom para a organização, pois o funcionário trabalha mais e melhor. No Brasil, sua utilização ainda esta sendo adequada às organizações e poucas já tem políticas próprias para essa utilização. (OLHAR DIGITAL, 2012)

O BYOD é um fenômeno e para sua utilização é necessário regras e processos que devem ser implementados pela gestão de segurança da informação. Com sua utilização crescente, as vulnerabilidades que podem ser atacadas também se tornam crescentes, para garantir proteção nos dados que circulam nas organizações, prevenindo atos maliciosos, estas tendem a reestruturar suas áreas e setores de trabalho, focando em suas políticas de utilização.

As políticas devem ser seguidas e respeitadas com rigor por seus colaboradores, mas muitas vezes as organizações não sabem quais políticas devem implantar, como devem ser implantadas e como conscientizar seus colaboradores para boas práticas de utilização do fenômeno BYOD.

A grande preocupação das organizações esta voltada à segurança de suas informações, pois caso estas se percam, ou sejam roubadas, por perda de um aparelho, utilização indevida ou furto do mesmo, as informações podem ser utilizadas de maneira imprópria, prejudicando a organização ou o responsável pela informação.

A organização deve estar preparada para lidar com esse tipo de situação, pois dependendo do valor das informações, esta pode sofrer falência ou grande prejuízo. Para isso, é necessário que a equipe de TI tenha de prontidão políticas de bloqueio de aparelhos, para que se possa bloquear o acesso às informações. (PESSOA, 2013)

Muitas organizações estão interessadas em utilizar o BYOD, devido aos aspectos de custo e desempenho, porém estas não adequaram políticas para que essa utilização não cause prejuízos ou problemas futuros.

Com base na fragilidade cometida pela maioria das organizações na falta de uso de políticas de segurança, principalmente as de pequeno porte e com interesse em conhecer políticas de segurança da informação em organizações que já as utilizam, este trabalho voltou-se para a seguinte questão:

Como uma organização pode adequar suas políticas de segurança da informação, considerando o fenômeno BYOD?

Foram analisadas e destacadas políticas que poderão ser utilizadas nas organizações que optaram aderir ao fenômeno BYOD, explicitando quais atitudes podem causar perda de informações e como a gestão de segurança da informação deve se relacionar com a política a ser implantada na organização.

Essa obra teve como objetivo geral mostrar as melhores práticas a serem implantadas nas organizações e como as vulnerabilidades ocorrem, quais as causas e como atingem a maioria dos dispositivos.

Metodologia de pesquisa

No desenvolvimento deste trabalho foram utilizadas pesquisas exploratórias através de dados bibliográficos, aprofundando o conhecimento com embasamento teórico em políticas e normas voltadas para a segurança da informação. Como esclarece Fontes (2012, p.3) “A informação possibilita o conhecimento da organização. Este conhecimento é a base para a geração de valor nas corporações”.

Como forma de embasamento prático em contextos reais, foi efetuada entrevista com o especialista na área de políticas de segurança da informação e professor da Fatec, Edson Gaseta. Conforme Wazlawick (2009, p. 40) “Assim, deverá ser suficiente trilhar o caminho descrito pelo método para se alcançar o objetivo”.

Sendo assim, com a coleta de informações voltadas para BYOD já utilizadas em organizações, foi possível conhecer um exemplo de aplicação em uma organização, como essas políticas são cumpridas pelos colaboradores, quais são as dificuldades para prática do BYOD, as vulnerabilidades que ocorrem e como são monitoradas.

Por fim, uma vez percorrido todo esse percurso metodológico e tendo este roteiro como base, a titulo de contribuição, este trabalho apresenta propostas de documentação, distribuição de tarefas entre setores e um *checklist* com os principais aspectos da segurança da informação que devem se fazer presentes na política de BYOD em uma organização. Vale salientar que a elaboração dessas propostas teve como fonte principal a triangulação dos dados aqui coletados através dos diferentes mecanismos metodológicos.

2 SEGURANÇA DA INFORMAÇÃO

Segurança da Informação é um tema recorrente em um mundo em constante mudança. A informação é um ativo muito valioso para a organização e deve ser cuidado. De acordo com Fontes (2006, p.11) segurança da informação é:

> "Um conjunto de orientações, normas, procedimentos, políticas e demais ações que tem como objetivo proteger o recurso informação, possibilitando que os negócios da organização sejam realizados e sua missão seja alcançada".

As informações de uma organização são bases para a estrutura do negócio e devem sempre estar asseguradas de maneira adequada e com verificação periódica.

> "Se a organização tem a oportunidade de conhecer toda a informação valida sobre a sua situação de proteção do recurso informação valida sobre a sua situação de decidir livremente pela solução mais adequada para ela naquele momento"(FONTES, 2008, p.22).

Para assegurar que as informações estarão protegidas, os ambientes e os equipamentos utilizados para seu processamento, seu armazenamento e sua transmissão devem ser protegidos. Todos na organização devem estar cientes da importância das informações em questão. "A informação, independente de seu formato, é um ativo importante da organização". (FONTES, 2006, p.1).

Toda informação transmitida ou recebida dentro da organização deve ser controlada, porém esta deve estar ciente que para esse controle de fluxo das informações trafegadas e terá que verificar quanto esta disposta a desembolsar para assegurar e controlar suas informações. Para isso a organização deverá analisar se o impacto de um ataque ou invasão será alto, baixo ou mediano, qual será o nível de necessidade de segurança.

Conforme destaca Fontes (2006, p.2), a "informação é muito mais que um conjunto de dados, transformar esses dados em informação é transformar algo com pouco significado em um recurso de valor para nossa vida pessoal ou profissional".

É necessário entender que, a informação é um bem muito importante na vida do ser humano, pois a vida gira em torno de informações, tudo o que o ser humano precisa fazer, faz ou até deixa de fazer é devido a uma informação que obteve por algum meio, mas as informações nem sempre são vistas com a devida importância.

No caso das organizações, muitas ainda não sabem o valor que suas informações têm e não assegurando estas da devida maneira, traz riscos de perdas ou de transmissões indevidas, causando prejuízo à organização, em alguns casos, falência. Vale salientar que é impossível obter segurança total de todas as informações.

Não há situação certa ou errada, cada organização deve saber qual será a solução mais adequada para assegurar suas informações. Em alguns casos pode não ser a melhor solução, mas a que mais se encaixa nas necessidades da empresa. Porém é possível destacar alguns requisitos primordiais para assegurar a informação, conforme figura 1, são eles:

Figura 1 - Requisitos de Segurança da Informação

Fonte: Autoria própria.

Integridade: asseguram que os dados não sejam modificados ou excluídos sem autorização, que continuem com os mesmos aspectos de sua ultima utilização. As características da informação devem estar

armazenadas com o formato original, estas devem ser protegidas e acessadas somente por pessoas autorizadas (FERREIRA; ARAUJO, 2008, p.44)

Confidencialidade: esta destaca o valor da informação e caracteriza-se pela garantia de que essa informação só será acessada pelo usuário autorizado, as informações não devem ser transmitidas a qualquer pessoa, caso isso ocorra, poderá acarretar prejuízo para empresa ou danos para uma pessoa física. (FERREIRA; ARAUJO, 2008, p.44)

Disponibilidade: garantia de que a informação estará disponível para uso de pessoas autorizadas, deverá estar de acordo com a legislação e ser auditada. Os dados devem ser confiáveis e de fácil acesso. (FERREIRA; ARAUJO, 2008, p.44)

Autenticidade: tem por base proteção das informações após o envio, garantindo que esta não seja modificada na comunicação e transmissão ao remetente, preservando também a identidade do remetente. (SILVA NETTO; SILVEIRA, 2007, p.377)

Mesmo com os aspectos mencionados, as informações se perdem ou sofrem furtos e danos devido à falta de comprometimento e uso indevido de ferramentas disponibilizadas, na maioria das vezes pelo mau uso da *Internet*. Devido a isso, é necessária a implantação da gestão de segurança da informação, que será responsável por controlar os recursos utilizados dentro da organização.

2.1 Gestão de segurança da informação

Como já mencionado, a informação é requisito primordial para o bom funcionamento dos negócios dentro da organização. Nos dias atuais, se vê o crescente número de ataques e roubos de informações por crackers e fraudes eletrônicas, através da invasão de privacidade. (FONTES, 2008. p.185)

Para melhor precaução com a segurança da informação, toda organização deve ter um setor de Tecnologia da Informação (TI) bem estruturado que trabalhe em conjunto com a gestão de tudo que se refere à informação, implantando processos para proteção das informações em todas as áreas da organização, de maneira adequada.

As organizações podem optar por deixar responsáveis pelas informações os próprios colaboradores, sendo estes, conscientes por todas as informações que transmitem e recebem, verificando a melhor maneira de utilização dos requisitos disponibilizados para realização de suas atividades.

Definir um gestor em cada área da organização pode ser uma opção, sendo este, o responsável pela transmissão e recebimento de dados, acessos efetuados e outras ações realizadas pelos colaboradores que trabalham com os dispositivos móveis ou desktops, ou seja, por toda forma de acesso ao sistema e atividades exercidas.

São poucas as organizações que tem um setor dedicado à gestão de segurança da informação, porém algumas já adequaram esta área, que coloca uma pessoa responsável por todo o trafego de informações e acessos dentro da organização, adequando políticas e regras a serem implantadas para isso.

O gestor precisa ter ampla visão de toda a organização e todas as atividades nela realizadas, com o conhecimento vasto e uma pessoa dedicada à gestão de segurança da informação, a implantação de políticas se torna mais criteriosa e especifica. (FONTES, 2008, p.179)

O gestor é a pessoa que tem autoridade para liberar e negar acessos aos usuários ou determinar qual informação pode ser acessada por quais funcionários. Ele deve ter ciência do seu posicionamento, não deve liberar acesso às informações por amizade ou afeição, ou deixar de efetuar liberações por falta destes. Para isso, o gestor deve analisar se o funcionário realmente precisa do acesso ou da informação em si, qual o nível de acesso que cada funcionário deve obter (escrita, remoção, leitura ou criação). Conforme Fontes (2006, p.39):

> "O gestor deve estar atento e garantir que cada usuário tenha apenas o tipo de acesso necessário para o desempenho de sua função profissional dentro da organização, com isso é possível operacionalizar a liberação de informação".

A liberação deve ficar registrada e ser evidenciada para que, caso seja necessário no futuro, haja documentação informando responsável pela liberação e motivo pelo qual foi efetuada. (FONTES, 2006, p.38)

O gestor deve garantir que as mudanças que possam ocorrer sejam planejadas, controladas e analisadas, de modo que não interfiram na organização de maneira prejudicial. Deve controlar os problemas ocorridos, identificando-os inicialmente, registrando e acompanhando com uma análise criteriosa para resolução do mesmo, de maneira adequada utilizando ações preventivas, detectivas e corretivas.

Com a área de gestão de segurança da informação implantada na organização, o gestor deve executar níveis de proteção das informações, de modo que diminua riscos de problemas futuros, esses níveis de informações podem ser classificados por prioridades, por exemplo, as informações que circulam no departamento financeiro e compras são de máxima prioridade de segurança. Informações da área de logística e atendimento tem a segurança de suas informações com prioridade normal e informações que não

poderiam prejudicar a organização caso vazassem, como: cronogramas, avisos, datas especiais, entre outras, podem ser tratadas com baixa prioridade.

A informação deve ser assegurada não só por meios tecnológicos, mas pelo próprio usuário, a segurança da informação deve se encaixar de maneira que conscientize o usuário a não transmitir informações indevidamente, seja por meios tecnológicos ou até mesmo por conversas pessoais.

A conscientização tem como dever lidar com a obediência profissional, pois cabe ao colaborador transmitir ou não as informações de maneira correta, tornando este peça chave no armazenamento de informações. O ideal é adotar roteiros e normas para que além da conscientização de uso das informações, também fique claro o dano que poderá ser causado caso as políticas sejam desobedecidas. Essa conscientização faz com que o usuário tenha comprometimento com as informações obtidas. (FONTES, 2008.p.186)

2.2 Normas e roteiros para gerenciamento da Segurança da Informação

Os procedimentos e boas práticas para gerenciamento de serviços de TI abordam esses serviços durante todo o seu ciclo de vida para que o gerenciamento seja realizado de maneira adequada em todos os seus níveis, possuindo uma visão voltada para a alta qualidade de serviços na origem e na entrega. (MOSENA, 2015)

ITIL

A organização pode aderir à utilização do *Information Technology Infrastructure Library* (ITIL), que por sua vez, trata-se um roteiro de boas práticas para auxilio a gestão de segurança da informação na implantação de normas e regras em suas políticas de segurança da informação, conduzindo processos nas atividades da organização. (FONTES, 2008, p.138)

O ITIL foi criado pela *Office of Government Commerce*/UK, utilizado para ligação entre organizações britânicas. Suas implementações em muitas organizações são bem aceitas por não terem nenhuma plataforma proprietária, ser de fácil entendimento e poder ser aplicada em qualquer empresa, de qualquer segmento. (CUNHA; CASTRO, 2014. p.36)

Para Ferreira e Araujo (2008, p. 65) o ITIL é utilizado em diversos países por qualquer tipo de organização e “pode-se ousar dizer que a ITIL é o padrão mundial no Gerenciamento de Serviços”. Este disponibiliza certificações com vários níveis, no avançado pode-se gerenciar o TI em uma organização, sua versão mais recente é V3, no Brasil existem poucos especialistas em ITIL.

Os critérios devem ser estabelecidos em todas as áreas de uma organização para melhores práticas. Uma grande preocupação das organizações são os gastos na área de TI, estes gastos são grandes e devem ser controlados com ajuda do ITIL, não somente os gastos em TI, mas em todas as áreas devem ser controlados. Para que isso ocorra, a infraestrutura de TI na organização deve estar impecável e todas as datas de entregas dos relatórios de controles e analises devem ser seguidos com responsabilidade. (MANSUR, 2009)

O ITIL baseia-se em estratégias, projetos, transições, operações e melhorias continuas de serviços, aonde são vistas as necessidades da organização. Cada uma dessas características carrega responsabilidades em mudanças, implementações, soluções requisitos em que devem ser adotados. (MUNDO ITIL, 2015)

Figura 2 - Ciclo ITIL

Fonte: MUNDO ITIL, 2015.

É de extrema importância que o ITIL consiga alinhar a organização com suas necessidades em questão, para isso, ele deve propor efetividade nos serviços realizados, diminuir a quantidade de gargalos que possam ocorrer, acompanhar e, se possível, aumentar o ciclo de vida da tecnologia implantada na organização. Com esses aspectos é possível que haja maior satisfação entre os clientes e colaboradores, redução de custos, minimização de problemas sistêmicos e melhor entendimento dos processos implantados. O profissional deve se adequar ao nível de necessidade da empresa, com isso é possível seguir características aplicadas na organização, (MANSUR, 2009).

O profissional qualificado em ITIL poderá ser admitido de acordo com o nível de exigência da organização, este tem obrigação de gerenciar e propor boas práticas e estratégias. Ele fica responsável também pela gestão em TI, onde são efetuados os planejamentos dessas estratégias de treinamentos, controles e analises, de modo que haja preocupação com a economia de custos que as estratégias propõem, com o cumprimento do que se é planejado e com um bom ambiente de trabalho. (MOSENA, 2015)

ISO 27001

Para as normas impostas dentro da organização, a ISO 27001 é padrão de utilização em gestão e gerenciamento de segurança da informação. Sua utilização caracteriza a organização como confiável, oferecendo maior segurança para os clientes que com ela trabalham e podendo ser utilizada em qualquer tipo ou porte de organização. Qualquer organização que queira utilizar a ISO 27001 deverá ter uma certificação, onde a unidade certificadora confirma a utilização da ISO na organização. (ISO 27001, 2013)

Proveniente da BS7799 (British Standards) publicada pela *International Standardization Organization* (ISO) em 2005, a versão mais utilizada é a ISO 27001 e foi publicada em 2013.

Esta também tem sido melhorada ao passar dos anos, auxiliando as organizações a mitigarem riscos causados por vulnerabilidades ocorridas. (ISO 27001, 2013)

Toda organização que trata informações em seus dispositivos e as transmite para fora da própria organização deve trabalhar com o SGSI, sistema de gerenciamento de segurança da informação que segue as normas da ISO 27001. (ALMEIDA, 2013) Com o SGSI amparado pela ISO 27001, a organização poderá usufruir das melhores técnicas para controles e monitoramento, envolvendo recursos humanos e tecnológicos.

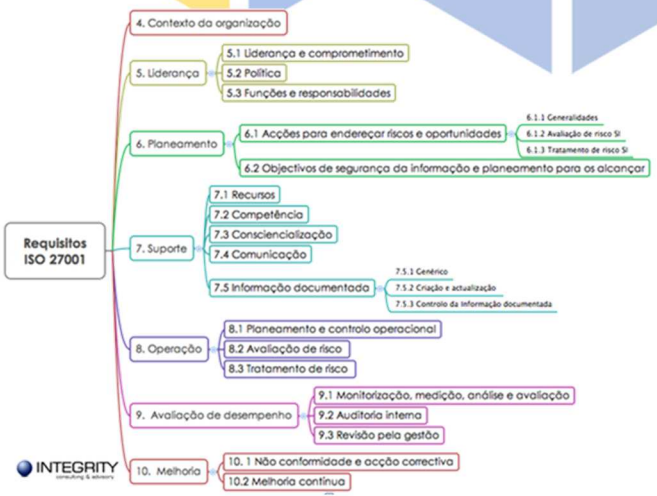
O SGSI busca definir critérios, termos e objetivos para boas práticas dentro da organização, para isso, verificam quais são suas necessidades, auxilia para analise de contratos e regulamentos já implantados na organização. (ABNT, 2011, p.4)

É necessário que haja treinamento apropriado referente ao SGSI para todos os colaboradores na organização, porém, direcionando os aspectos a serem seguidos para cada área de trabalho, conscientizado os colaboradores e esses treinamentos devem ser registrados. (ABNT, 2011, p.10)

O processo mencionado acima auxilia na avaliação das normas que estão sendo seguidas pelos colaboradores, identificando e avaliando riscos, ameaças e vulnerabilidades que possam ocorrer e seus níveis de impacto no desempenho diário das atividades na organização. (ABNT, 2011, p.5)

A ISO tem em sua composição a determinação de regras e condições para utilização das normas, para melhor identificar, a figura 3 apresenta um diagrama expondo sua utilização: (ABNT, 2013)

Figura 3 - Diagrama de Requisitos ISO 27001



Fonte: Integrity, 2015.

A figura 4 mostra os controles que geralmente são impostos na organização, conforme sua precisão:

Figura 4 - Controles impostos pela ISO 27001 na organização

Fonte: Integrity, 2015.

A ISO 27001 oferece diversos benefícios em gestão de segurança da informação para boas práticas organizacionais, como por exemplo, a proteção das informações tratadas, obtendo os maiores padrões de gestão de segurança e trazendo maior sigilo em suas informações. (ABNT, 2013)

Diante de problemas que possam ocorrer mesmo com o uso das normas, a organização também deve obter um roteiro com ações que deverão ser utilizadas. Essas ações auxiliam na resolução desses problemas, minimizando assim falhas que ocasionam preocupações a organização.

2.3 Ações para auxilio na obtenção de segurança da informação

Com toda a informação que circula nas organizações regendo suas atividades diárias, erros podem acontecer, uma informação pode ser transferida a uma pessoa sem autorização, pode haver invasão, furto de informações ou falhas nos dispositivos móveis e equipamentos utilizados para essas atividades. A organização deve se atentar e se enquadrar com ações para prevenir ou solucionar esses tipos de acontecimentos que comprometerão a segurança de suas informações, sendo estas as principais:

Ações preventivas: efetuadas antes de o problema ocorrer. Podem ser implementadas normas no dia-a-dia ou a utilização de antivírus. É de responsabilidade da área de TI trabalhar com ações preventivas nas máquinas, equipamentos ou dispositivos utilizados na organização, como por exemplo, a verificação mensal, a fim de prevenir que estes equipamentos apresentem problemas futuros atrapalhando o desempenho do fluxo de atividades, isso ocorre com invasões ou até mesmo, caso o dispositivo e equipamento esteja obsoleto. (FONTES. 2006. p.53)

Ações detectivas: são utilizadas quando não a ação preventiva não foi realizada para detecção de falhas ou riscos identificados. Servem para detectar e solucionar os problemas com maior agilidade, para efetuar a ação corretiva. Um exemplo que mostra claramente uma ação detectiva é a quantidade de tentativas de *login* por meio de senha, o ideal é que seja criado bloqueio do usuário após certa quantidade de tentativas. (FONTES. 2006. p.54)

Ações corretivas: para quando o problema ocorreu e não foi evitado com as ações mencionadas anteriormente. Neste ponto, o problema já foi detectado e esta afetando o equipamento ou desempenho de atividades dentro da organização, causando danos à mesma.

Seu objetivo é minimizar os problemas ocorridos, corrigindo-os para que as atividades realizadas no negócio não sejam prejudicadas em grandes proporções e sejam retomadas em curto prazo. As cópias de segurança são exemplos de ações corretivas. (FONTES. 2006. p.54)

Não há necessidade de fazer cópias de todos os arquivos, mas sim, dos mais importantes que afetarão na continuidade das atividades exercidas no negócio. Fontes (2006, p.46) menciona que “toda informação deve ser avaliada em relação à sua criticidade e, consequentemente, em relação à necessidade de existência de cópias de segurança”.

As cópias de segurança devem ficar salvas no servidor ou em mídias como fitas de *backup* periódico e podem ser efetuados automaticamente em datas agendadas pelo TI O ideal é que seja feita mais de uma cópia e estas devem ser guardadas em lugares distintos e de acesso somente por pessoas autorizadas, garantindo o mínimo possível do risco de perda. (FONTES. 2006, p.45)

Qualquer ação tomada para corrigir um erro, prevenir um roubo ou simplesmente uma ação de rotina que monitore os equipamentos e transmissão de informações deve ser organizada e documentada através das políticas de segurança da informação impostas na organização.

3 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Com a dependência do ambiente de TI para grande parte das atividades exercidas, as organizações requerem melhor infraestrutura, para que se possa tratar os quesitos disponibilidade, quantidade e qualidade corretamente. (FERREIRA; ARAÚJO, 2008, p.65)

Para isso, 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. (FERREIRA; ARAÚJO, 2008)

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 e rege o negócio. Devido a isso, devem estar asseguradas de maneira rigorosa. Cabe ao funcionário à responsabilidade de assegurar a informação que lhe é transmitida.

Falando em pessoas, na grande maioria das organizações, os maiores infratores são os que demonstram ser mais confiáveis. Quando a fraude vem de um funcionário de baixa hierarquia, é mais fácil de ser resolvida, pois haverá setores de monitoramento para identificar tal fraude e facilmente identificará o fraudador, ao se tratar de um cargo de alto nível, a dificuldade no monitoramento da fraude se torna mais difícil, pois dependendo do cargo não há monitoramento para o mesmo e o ato malicioso pode passar despercebido ou dificultar a obtenção de prova de que tal pessoa cometeu a fraude. (DAWEL, 2005. p.66)

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. (FONTES, 2008. p.219)

No caso de necessidade, o maior fator é dinheiro, levando o funcionário a fraudar a organização, roubando informações ou equipamentos. Por oportunidade, 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, 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. (FONTES, 2008. p.9)

Deve existir uma política principal documentada de simples entendimento para que os colaboradores consigam tratá-la com responsabilidade e a sigam corretamente.

> “Para se ter uma estrutura adequada, recomendo que deva existir uma política principal, descrita em um documento curto e simples de forma que todos os usuários entendam facilmente como a organização deseja que a informação seja tratada e quais são as principais responsabilidades dos usuários. Outros documentos, tipo políticas específicas e normas, podem e devem complementar esses requisitos básicos”. (FONTES, 2008. p.9)

O funcionário deve estar ciente das consequências para ele e para a organização, caso ele haja de maneira ilícita ou não tenha cuidado com a maneira que trafega as informações, sendo assim. É necessário, orientar o funcionário de sua responsabilidade, para que um ataque não ocorra em função de descuido. (FERREIRA; ARAUJO, 2008. p.187)

Devem-se conter também requisitos básicos, como definição de regras, responsabilidades, obrigações e procedimentos aplicados a todas as áreas da organização. Sem regras ou normas, são possíveis ocorrências de ataques maliciosos causados por ameaças.

A ameaça é um evento que explora as vulnerabilidades e seu controle pode ser criado através de uma planilha, caracterizando suas maiores fontes, motivações e ações. Deve-se ser efetuado controle de verificação periódico, a fim de que sejam detectadas antes de serem exploradas. (Apêndice A)

Os ataques podem ser por erros humanos, falhas de hardware ou software, vandalismo, acessos indevidos, ações da natureza, entre outros. No controle avaliam-se os maiores índices de quebra de

segurança que causam essas ameaças. Para que a ameaça seja concretizada, esta deve explorar a vulnerabilidade, sem essa exploração a ameaça não tem tanto valor. (Apêndice A)

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. (FERREIRA; ARAÚJO, 2008. p.177 e 178)

Pode-se dizer que há possibilidade da ameaça explorar a vulnerabilidade, essa possibilidade é chamada de risco, esses riscos podem prejudicar a organização, gerando prejuízos caso ataque um ativo de grande importância, devido à falta de monitoramento. Para identificar os riscos é preciso caracterizar quais são seus componentes, as consequências caso sejam examinados e como irá impactar nos negócios da organização. (Apêndice A)

A gestão de riscos efetua uma análise desses riscos que possam surgir dentro da organização e quais suas principais causas. Os riscos podem ser aceitos, definidos, analisados e monitorados. A gestão de riscos também fica responsável pela estimativa de riscos, aonde mostram os níveis de criticidade em cada um que for identificado. Com ela é possível evitar que os riscos ocorram dentro da organização. (GASETA, 2015)

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. (FERREIRA; ARAUJO, 2008. p.171)

3.1 Política de autenticação do usuário

Segundo Fontes, (2006, p.25) a política de autenticação do usuário é utilizada para fim de comprovação de acesso a sistemas e transmissões de informações. Pode ser considerada uma política essencial para segurança da informação. Fontes (2008, p.117) também menciona que “A autenticação de pessoas ou recursos é umas das ações mais difíceis no processo de segurança da informação”.

Algumas organizações tendem a utilizar autenticação por senha, com baixo custo e de resolução rápida e eficaz se torna a opção preferida. Existem outras opções de autenticação, como o cartão ou crachá, com nível de solução acima da senha. Pode-se utilizar também a biometria, que por sua vez, é a de maior custo e a solução mais eficaz, pois com esta opção somente a pessoa com a biometria cadastrada terá acesso às informações. (FONTES, 2008, p.147)

Os requisitos de biometria e cartão não se enquadram na utilização de dispositivos móveis e *notebooks*, pois ainda são poucos os que utilizam a autenticação biometria. As senhas ainda são o requisito de autenticação mais utilizado por poderem ser utilizadas em qualquer dispositivo ou *desktop*.

Apesar de sua facilidade, cabe ao usuário criar a senha, sua criação deve ser atenciosa e seguida por orientação para que seja de forte segurança, uma senha fraca pode ser furtada ou descoberta sem muito esforço. Muitos funcionários e usuários utilizam senhas padrões, repetidas ou com sequencias obvias de números, datas de aniversário próprio ou de alguém especial ou próximo, ajudando os infratores na descoberta da senha. (FONTES. 2006, p.25)

Alguns parâmetros conhecidos de criação de senhas são incentivados para todos que utilizam o sistema, são estes: primeira letra de cada palavra em uma frase que o usuário lembre com frequência, mistura de números e caracteres, utilização de no mínimo seis posições e mais importante, não deixar a senha gravada ou de fácil acesso para pessoas não autorizadas. (FONTES. 2006, p.25)

Para adequar a autenticação de usuário em dispositivos móveis pessoais e *notebooks*, as organizações devem ter um sistema de controle de autenticação do usuário para conexão a rede corporativa, para aplicativos que podem ser criados e implantados e para a utilização dos sistemas da corporação em smartphones e *tablets*, também podendo utilizar *login* e senha.

Para acesso as informações mantidas em nuvens, a organização pode atribuir autenticação também de *login* e senha para que este tenha acesso somente às informações autorizadas.

A desvantagem da utilização de senhas é o fato de o usuário demorar a decorar as senhas utilizadas para os recursos que necessita ou utilizar senhas obvias, fazendo com que as informações fiquem vulneráveis. (FONTES, 2008, p.147)

Tratando-se de dispositivos móveis e notebooks pessoais, deve contar com a conscientização dos funcionários na utilização de seus dispositivos móveis, sendo necessárias recomendações e treinamentos. A implementação de políticas devem ser especificas para BYOD, podendo implantadas, auditadas e exigidas.

4 CONSUMERIZAÇÃO E O FENÔMENO BYOD

Antes de adentrar no tema BYOD, faz-se importante a compreensão do cenário atual da indústria de eletrônicos, movido atualmente por uma tendência chamada consumerização.

4.1 Consumerização

De acordo com DODT (2013), a “consumerização é a tendência que tecnologias desenvolvidas com foco no mercado consumidor adentrem a esfera corporativa.”

A consumerização tomou notoriedade com o grande crescimento do mercado de consumo, onde os fabricantes se viram obrigados a criar aparelhos eletrônicos para uso residencial e disponibiliza-los a um valor menor que os aparelhos para uso comercial. (SHIBATA, 2012, p.3)

A consumerização quebra o paradigma para a inovação tecnológica, onde os equipamentos antes eram fabricados primeiramente para fins militares, em segundo lugar para consumidores pelo mercado de grande porte e só por último para o consumidor final em grande escala. Com o passar dos anos, a direção da fabricação dos equipamentos começou a ter destino contrário, sendo primeiro para o consumidor final, mercado de grande porte e fins militares. CASTRO e SOUZA (2015 p.3, apud Stagliono, Dipaolo, Coonely, 2013)

Conforme GARANHANI (2013, p.10) a 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 aonde incluem *smartphones, tablets* e *notebooks*.

A consumerização está envolvida com a evolução em TI, aproximando o consumidor final de novas tecnologias em dispositivos móveis, fazendo-os se adequarem as mudanças constantes e consequentemente levando seus dispositivos móveis para as organizações onde trabalham e passam maior parte do tempo. (STAGLIANO; DIPAOLO; COONELLY, 2013, p.8)

“A Consumerização de TI alterou o cenário das inovações tecnológicas no decorrer dos anos, proporcionando uma situação onde os consumidores possuem acesso as últimas tecnologias disponíveis, invertendo a lógica anterior, que dizia que a inovação chegava primeiramente aos ambientes corporativos.” (STAGLIANO; DIPAOLO; COONELLY, 2013, p.33 e 34)

A consumerização de TI é abordada por alguns autores como tendência de utilização de dispositivos móveis dos funcionários nas corporações. “Consumerização de TI é a tendência de permitir que os funcionários usem seus dispositivos pessoais para se conectar a recursos corporativos.” (STAGLIANO; DIPAOLO; COONELLY, 2013, p.36)

Em um contexto pessoal, a consumerização auxilia os consumidores a escolherem marcas de seus dispositivos móveis e equipamentos, para que estes se adéquem as suas necessidades e permitam que os consumidores tenham as informações estão sempre acessíveis. (STAGLIANO; DIPAOLO; COONELLY, 2013, 2013, p.4)

Visando as atividades exercidas internas e externas dentro das organizações, a utilização dessas novas tecnologias possibilita maior acesso as informações e considerando os benefícios às organizações provocados pela consumerização, outro fenômeno surge com força no meio corporativo: o BYOD.

O BYOD tem relação direta com a consumerização, afinal, uma vez que os produtos eletrônicos estão mais acessíveis ao usuário comum, é esperado que este queira utilizar seu próprio dispositivo no dia a dia de seu trabalho. (SILVA, 2012)

4.2 BYOD

O fenômeno "*Bring Your Own Device*" ou “Traga seu próprio dispositivo” (BYOD) disponibiliza a utilização de dispositivos móveis, ou seja, *smartphones, tablets* e *notebooks* nas corporações, esse fenômeno tem tomado grande proporção. Com o BYOD além de dados pessoais, os colaboradores acessam dados da organização, tendo em suas mãos informações quando precisarem. (PESSOA, 2013)

A utilização do BYOD tem o intuito de deixar os funcionários mais “livres” em relação a suas rotinas de trabalho, trazendo mais entusiasmo e talento se comparado a uma rotina de afazeres dentro na empresa em um *desktop* e mesmo que o trabalho seja dentro da empresa, o colaborador pode ter o serviço de *Internet* disponível o tempo todo de trabalho, sem custos adicionais em organizações com TI estruturada. Com isso, os colaboradores acabam trabalhando por mais tempo, muitas vezes sem questionar. (MORETTI, 2013)

No Brasil podemos citar duas grandes organizações que já trabalham com o BYOD, são elas IBM e Cisco Brasil. Segundo Ghassan Dreibi Junior, gerente de desenvolvimento de negócios de Borderless Networks da Cisco do Brasil "Os profissionais se sentem mais à vontade e produtivos porque podem usar os dispositivos que preferem, e não os que estão disponíveis dentro do ambiente de trabalho”. (OLHAR DIGITAL, 2012)

Tendo em vista benefícios para a organização, o custo é menor e o colaborador pode acessar as informações de qualquer lugar. (MORETTI, 2013) A produtividade aumenta com a utilização do fenômeno BYOD, podendo este ser utilizado até no fim de semana. (STAGLIONO; DIPAOLO; COONELLY, 2013, p.7)

Um exemplo a ser mencionado como aumento de produtividade com o BYOD é utilização em hospitais aonde o médico para aprovar um exame a ser feito, precisava ir a um *desktop* e autorizar o exame pelo sistema. Com o BYOD é possível essa autorização de exames pelo próprio dispositivo móvel do médico ou enfermeiro. (MARSHALL, 2014, p.14)

As desvantagens na utilização do BYOD acercam a segurança de informações, com o BYOD, abre-se um leque de equipamentos e sistemas operacionais diferentes, tornando mais trabalhoso à utilização da rede, sendo que, com um gerenciamento de rede inadequado, devido a essa grande quantidade de dispositivos móveis e sistemas operacionais diferentes, sem a devida implementação, pode-se comprometer a confiabilidade das informações transmitidas. (MUNIZ JUNIOR, 2013 p.16)

Outra desvantagem é a acarretada pela má utilização do colaborador, conscientemente ou inconscientemente, pode causar prejuízo à organização. Conforme menciona Moretti (2013) "... a maioria das empresas, que permite a prática de BYOD, exige que os funcionários tenham *softwares* de segurança instalados para prevenção de eventuais danos." A fim de garantir a segurança de suas informações.

A grande preocupação no BYOD é a segurança de informações, caso a informação se perca por má utilização do colaborador, conscientemente ou inconscientemente, pode causar prejuízo à organização. Conforme menciona João Moretti (2013) "... a maioria das empresas, que permite a prática de BYOD, exige que os funcionários tenham *softwares* de segurança instalados para prevenção de eventuais danos." A fim de garantir a segurança de suas informações.

Para que as informações não se percam, ou sejam utilizadas de maneira indevida, são necessários investimentos, fazendo com que esse aspecto seja melhorado. As organizações devem investir um custo alto em tecnologia e treinamento de pessoal, conscientizando os colaboradores referentes à importância das informações que acessam de seus dispositivos móveis. (MORETTI, 2013)

Muitas organizações agregam as suas políticas, assinadas e documentadas, regras para proibição de utilização de alguns aplicativos, recurso imposto pela gestão e política de segurança da informação, a determinação de proibição pode ser estabelecido devido à alta possibilidade de contaminação que um aplicativo pode trazer ao dispositivo. A gestão fica responsável por analisar esses aplicativos que podem se tornar prejudiciais. No caso de smartphones, o maior acesso para organização é para e-mails, já no notebook a utilização é para todos os fins.

Para que todos os colaboradores tenham as informações sobre o andamento das atividades exercidas dentro da organização muitas das organizações que trabalham com o fenômeno BYOD tem utilizado os arquivos em nuvem. Este meio é disponível e de fácil acesso para todas as pessoas dentro da organização, a utilização de arquivos em nuvem tem crescido de maneira significativa, pois, não é necessária utilização de um componente físico para armazenagem de arquivos e informações.

Pode-se usufruir das informações por qualquer sistema operacional de qualquer lugar. É possível o colaborador acessar os arquivos em nuvem utilizando o BYOD, ou seja, para que obtenha a informação desejada quando precisar e do local que precisar pelo seu dispositivo móvel, bastando apenas à utilização da *Internet*. (TAURION, 2012)

Após o surgimento do BYOD, surge o "*Bring Your Own Clouding*" ou "Traga Sua Própria Nuvem" (BYOC) tratando do armazenamento de informações para compartilhamento e sincronização, termo com especificações e propostas bem parecidas com as do *Cloud uting*. (TAURION, 2012)

A relação entre o BYOD e o *Cloud Computing* é direta, pois o BYOD traz o uso dos dispositivos móveis para dentro da organização, ou seja, trazendo mais flexibilidade para que as atividades da organização, quando optadas a serem realizadas através de *smartphones*, *notebooks* e *tablets*. Porém diferente do uso de desktops, que para obter a mesma informação precisavam estar ligados à mesma rede, tendo um servidor que armazenasse o banco de dados e fosse mapeado aos demais terminais, "dividindo" as informações, o *Cloud Computing*, disponibiliza os arquivos em nuvem, para uma visão simples, ele efetua um trabalho parecido com o exemplo dos computadores ligados a mesma rede, porém o *Cloud Computing* armazena as informações em nuvem, um local online, a utilização pode ser efetuada pelo acesso a um *e-mail* e o acesso às informações ficam disponíveis por qualquer pessoa que tiver *login* e senha e *Internet*.

Cloud Computing

Cloud Computing – "computação nas nuvens" ou "computação em nuvem", teve como um de seus desenvolvedores o pesquisador John McCarthy. (ALECRIM, 2008)

Figura 5 - Arquivos em Nuvem

Fonte: SlideShare, 2014.

O conceito nuvem foi retirado da ideia de que as informações não precisam necessariamente ser guardadas em um único local e seu armazenamento não pode ser divulgado a qualquer pessoa. Com o *Cloud Computing* não há restrições de locais de acesso, não é necessário armazenamento em um local fixo e é de fácil acesso em qualquer máquina com disponibilidade a *Internet*. (ALECRIM, 2008)

Interligado diretamente com o uso do BYOD, pois através do dispositivo móvel o colaborador poderá acessar as informações que precisa e se necessário, e com autorização, alterá-la e devolve-la a nuvem para o acesso de outro colaborador por outro dispositivo.

O fenômeno BYOB juntamente com o *Cloud Computing*, estão em evolução e implementação constante e tendem a aumentar cada vez mais, já que com estas, as atividades do negócio se tornam mais disponíveis e prazerosas para se trabalhar, então "é importante pensar sobre o quanto esse sistema pode ser vantajoso, já que o crescimento do uso de equipamentos móveis nas empresas é acelerado." (MORETTI, 2013)

Na organização, com o compartilhamento em nuvem, os funcionários podem acessar as todas as informações armazenadas em um único lugar, porém não em um componente fixo. (AMOROSO, 2012)

As informações podem ficar armazenadas em pastas nomeadas e modificadas por pessoas autorizadas, e é possível compartilhar as pastas com pessoas especificas, facilitando o armazenamento e acesso pelo dispositivo móvel de qualquer lugar, dentro e fora da organização.

Pode se citar um exemplo simples de utilização do BYOD com o *Cloud Computing*: Haverá uma reunião externa para apresentação do produto fabricado por uma organização que daremos o nome “X”, o funcionário responsável por apresentar o produto vai até a empresa “Y” que está interessada em adquirir o produto, lá o funcionário percebe que se esqueceu de um arquivo que continha informações importantes para atingir seu objetivo de venda. Pelo próprio *tablet,* ele acessa o arquivo em nuvem com *login* e senha, neste caso será citado o *OneDrive* (aplicativo da Microsoft, aonde é possível acessar on-line os arquivos armazenados) busca a pasta onde encontra-se o arquivo que precisa e baixa para seu *tablet* ou visualiza on-line, dispondo da informação no momento necessário.

A maioria das aplicações em *Cloud Computing* é gratuita, vantajoso para a organização e para o usuário, pois além de ser gratuita, em sua maioria, essas aplicações não dependem de um sistema operacional especifico, como mencionado anteriormente. Muitos aplicativos em *Cloud* oferecem serviços, além do armazenamento de arquivos, com algum deles é possível, ler, editar, compartilhar e tem seu próprio serviço de e-mail.

Os aplicativos em nuvem, na maioria das organizações, são utilizados como nuvens públicas, porém, podem-se utilizar também os aplicativos de nuvem privada, esses aplicativos tem o mesmo efeito comparado com os de nuvem publica, mas ficam em um ambiente corporativo através de uma infraestrutura adequada nas políticas de segurança das informações utilizadas na organização. Esse aplicativo é utilizado conforme as políticas dentro das organizações, para prevenir acessos de pessoas não autorizadas a suas informações. (ALECRIM, 2008)

Os custos com as nuvens privadas são mais elevados, porém são mais controladas e disponibilizadas conforme sua gestão de maneira mais eficaz. Sua implementação deve ser efetuada por uma equipe de TI especializada e conceituada, uma vez que implantada de maneira incorreta, esta pode gerar grande prejuízo para a empresa. (ALECRIM, 2008)

Nas aplicações em nuvens híbridas, informações mais criteriosas e importantes podem ser direcionadas as nuvens privadas, enquanto as informações de importância menor podem ser direcionadas as nuvens públicas. Também devendo ser monitorada e controlada pela gestão de segurança. (ALECRIM, 2008)

Mesmo com a implantação correta, a utilização dos arquivos em nuvem, seja por nuvem pública, privada ou híbrida, devem ser de uso consciente do funcionário. Para essa conscientização de utilização, é necessário que a organização realize treinamentos e se necessário contrato com clausulas de uso para esses aplicativos. (ALECRIM, 2008)

A organização deve dar suporte ao colaborador que utiliza o BYOD, porém também deve monitorar a utilização desses dispositivos. Os resultados desses monitoramentos são acompanhados junto à gestão de segurança da informação, que analisará falhas cometidas pelos colaboradores em relação às políticas aplicadas na organização.

Para monitoramento, algumas organizações utilizam o *Mobile Device Management* (MDM), ferramenta de gerenciamento utilizada para monitorar, controlar e identificar dispositivos e usuários, evitando que haja transmissões de informações indevidas. (MORETTI, 2013)

O MDM é um sistema que permite a organização e acesso a todas suas informações em tempo real, podendo monitorar e controlar os acessos e aplicativos que estão sendo executados, efetuar remoção ou instalação de arquivos de maneira remota entre outros aspectos que serão vistos mais a frente.

MDM

O *Mobile Device Management* (MDM) é um sistema de gerenciamento utilizado nas áreas de administração e gestão de segurança da informação e tem como objetivo cuidar do gerenciamento de dispositivos móveis. Com o MDM é possível controlar os acessos pelas redes wireless nas organizações e apagar todos os dados do dispositivo ou até desligá-lo.

Previne os acessos impróprios por dispositivos móveis através de filtros de acesso, se tornando indispensável caso a organização trabalhe com BYOD. Porém ele não esta ligado diretamente ao BYOD, uma vez que, os dispositivos não vêm com o aplicativo MDM instalados, é necessário que se proponha a utilização ou a enquadre nas políticas de segurança da informação da organização. (MUNIZ JUNIOR, 2013, p.30 e 31)

Sua utilização é remota e serve para minimizar riscos e vulnerabilidades que podem ocorrer dentro da organização, reduzir custos e prejuízos e tempo de inutilidade. Este é utilizado dentro das diretrizes de políticas de segurança da informação, seus relatórios auxiliam a organização nas decisões a serem tomadas. (GIORGI, 2014)

Podem-se mencionar algumas etapas de grande importância para a sua utilização, sendo elas: a configuração dos dados do dispositivo móvel pelo sistema MDM, de acordo com as políticas aplicadas; a distribuição dos aplicativos MDM nos dispositivos móveis e notebooks e a autenticação dos dados, uma das etapas de maior importância, deve ser executada após a instalação, enviando os dados (IMEI, endereço IP / MAC, número de telefone, etc.) para o servidor de MDM, comparando os dados do dispositivo com os dados registrados no sistema, garantindo a sua autenticidade. Também é possível trabalhar com comandos, como o de “limpeza remota” e controlar as ações do dispositivo móvel conforme as políticas impostas. (RHEE; JEON; WON, 2012, p.353 e 354)

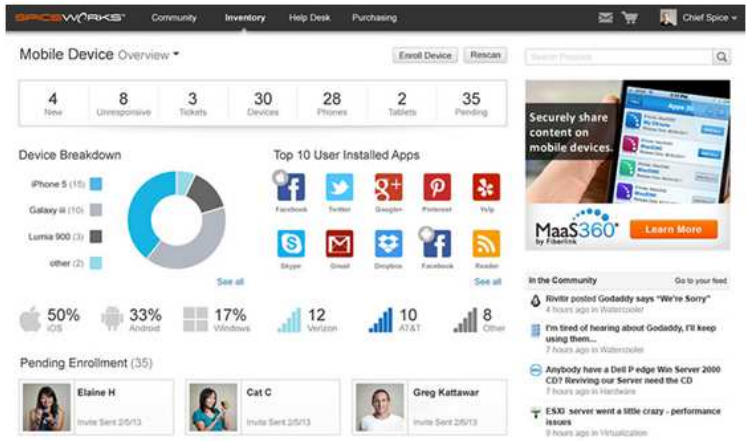
Para João Moretti (2013) o MDM "oferece condições de assegurar que os dados estejam protegidos em qualquer situação, até mesmo no caso de perda, extravio ou roubo dos dispositivos." Assegurando assim que as informações não se percam ou causem prejuízo à organização, já que todo o conteúdo de informações armazenados nos dispositivos é apagado em caso de perda ou furto do mesmo.

Existem *softwares* que podem ser baixados pela *Internet*, um exemplo é o MDM liberado para utilização no Windows Phone 8.1, permitindo o gerenciamento configurações do dispositivo, controlando fluxo de informações, protegendo mensagens de *e-mail* enviadas e recebidas pelo dispositivo Windows Phone 8.1. (MICROSOFT, 2015)

Existem outras empresas que disponibilizam *softwares* de MDM, em sua grande maioria, o *software* é custeado, algumas já informam o valor em seu site, como é o caso da Spice Works, que também disponibiliza o MDM gratuitamente, porém com menos recursos. Pode se mencionar como exemplos de empresas que também trabalham com MDM a Parallels e a Manage Engine, a cotação de valores pode ser solicitada pelo próprio site, onde também contém informes sobre seus *softwares*, especificando os recursos que oferecem.

Os recursos apresentados são geralmente os mesmos em diversas empresas, como limpeza de dispositivo, bloqueio, configurações, gerenciamento de políticas, gerenciamento de aplicativos, rastreio de dispositivos móveis, listas de bons e maus aplicativos, entre outros. A figura 6 é um demonstrativo oferecido pelo site da Spice Works como visualização de como é o sistema, com o intuito de propaganda, com a figura 6, é possível ter base de como o *software* se apresenta.

Figura 6 - Sistema MDM Spice Works



Fonte: Spice Works, 2015.

O MDM verifica toda e qualquer funcionalidade dentro do sistema da organização interpretando ameaças, riscos e vulnerabilidades, desde a instalação até a desinstalação de aplicativos. "Com certeza é um sistema que proporciona funcionalidades importantes para as companhias." (MORETTI, 2013)

Com essa plataforma de sistema é possível implantar políticas de segurança da informação com níveis de utilização, podendo classificá-las como alta, média e baixa. Cada colaborador terá acesso somente às atividades e informações que condizem a sua área de trabalho, evitando atos maliciosos por partes dos colaboradores.

5 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO PARA BYOD

As políticas de segurança que devem ser implantadas para BYOD não fogem muito das políticas já utilizadas pelas organizações.

Para obter boas políticas de segurança da informação, a organização pode unir o responsável de cada setor para acolhimento de informações junto ao TI ou gestão de segurança da informação, o sistema que irá implementar as normas a serem seguidas. Com os profissionais de cada área da organização trabalhando juntos, a organização consegue obter informações precisas e conseguem analisar as melhores praticas que se adéquam as suas necessidades. (FERREIRA; ARAUJO, 2008. p.37)

O TI se tornou área indispensável em uma organização e para a utilização do BYOD, essa área deve criar uma estrutura e planejamento com boas práticas para que consiga sanar todos os problemas que possam vir a ocorrer devido a sua utilização. (CUNHA; CASTRO, 2014. p.35)

Em empresas de pequeno porte, geralmente o próprio TI analisam as melhores políticas e regras a serem seguidas, com consentimento de um superior que aprove estas. Já em empresas de grande porte, a gestão de segurança da informação fica responsável por aderir, implementar e controlar essas políticas.

O TI independente do porte da empresa, é responsável pela implementação do BYOD, analisando acessos aos dispositivos, os vários sistemas operacionais que podem ser utilizados, como iOS e *Android* e dispositivos em si, como *hardware*. Segundo Debora Cocchi (2013, p.1)

> “uma política de segurança para aplicação BYOD deve ser estabelecida, onde serão definidos critérios de aceitação para o uso de dispositivos móveis particulares no ambiente corporativo.”

As políticas devem ser bem fundamentadas, aprovadas e formalizadas por documentação, elas serão desenvolvidas com auxilio das informações sobre aplicativos e sistemas mais acessados pelos colaboradores, entre outros aspectos que contribuem para o exercício das atividades no dia-a-dia recebidas pelo responsável de cada área da organização, mas esse é só o começo para se decidir como serão as políticas de segurança da informação a serem implantadas. (FERREIRA; ARAUJO, 2008. p.38)

Os procedimentos, pesquisas elaboradas para assegurar as informações e definir melhores estratégias, devem ser revisados e podem ser modificados com o tempo, mas é importante se manter datada e assinada desde sua aprovação e implantação até uma possível modificação. Com a aprovação da política, a organização deverá divulgá-la e explicá-la a todos que nela trabalham, para que não haja dúvidas. (FERREIRA; ARAUJO, 2008. p.40)

As informações devem recolhidas para que sejam efetuadas definições e verificações de políticas já criadas, quais são os fatores que motivam a criação dessas políticas. Após essa analise, são definidas as regras para acessos de informações para cada usuário de cada área da organização e como serão efetuadas

as auditorias. Outra preocupação são os procedimentos para descarte de dispositivos, armazenamento de informações e outros aspectos que devem ser regrados pelas políticas de segurança.

Para que seja vantajosa a utilização do BYOD no ponto de vista comercial, as políticas de segurança da informação devem ser integradas a organização por se tratar de diversos dispositivos e sistemas operacionais.

Um aspecto relevante é a privacidade do colaborador em relação ao seu dispositivo móvel, uma vez que este é utilizado para fins profissionais, mas ainda é de uso pessoal, contendo informações de cada colaborador, para isso, fica a critério da organização implementar regras documentadas em que os dispositivos móveis sejam gerenciados de maneira adequada para ela e o colaborador.

Conforme Pinheiro “deve ficar bem definido de quem é a propriedade do equipamento e os requisitos de segurança que o proprietário deve seguir”. Com isso, é possível afirmar que, é necessário haver controle de gerenciamento de informações pessoais e profissionais e o uso deste deve ser claro, sendo documentadas para fins jurídicos e impossibilitando problemas futuros para ambas as partes.

As organizações devem impor responsabilidades para a segurança, controlar ameaças e riscos que possam ocorrer através de relatórios de incidentes e uma gestão de continuidade de negócios, para que não precisem interromper nenhuma atividade da organização. (CUNHA; CASTRO, 2014. p.36)

As políticas podem implementar diversos recursos para garantir a segurança da informação, além dos aspectos citados acima, pode-se mencionar a criptografia das informações ou senha para acesso e em caso de perda do aparelho, as informações devem ser apagadas remotamente e se utiliza também o recurso de localização remota, essa localização remota ainda só está disponível em iOS da Apple. No *Android* para que se possa apagar conteúdos do dispositivo, é necessário que este tenha instalado um aplicativo para tal função, podendo ser este o MDM. Não existe 100% de eficácia garantida na segurança da informação, porém a como dificultar a invasão de ataques maliciosos. (GIORGIO, 2014)

6 ESTUDO DE CASO

As organizações que trabalham com o fenômeno BYOD precisam ter políticas para utilização correta deste, com base nas políticas de segurança da informação já utilizadas nas organizações, algumas já adequaram estas para o BYOD.

Neste trabalho foi realizada uma entrevista com o profissional na área de gestão de riscos, Edson Roberto Gaseta, a fim de compreender melhor o cenário atual em relação às políticas de segurança para BYOD.

Os dados da empresa citada pelo entrevistado são confidenciais e não foi possível autorização de uso destes, sendo assim, foi dado o nome fictício de “organização X” para que não comprometa o entrevistado.

Foram selecionadas algumas perguntas com base nessa utilização para as atividades diárias da organização disponíveis no apêndice A.

7 ANÁLISE DA ENTREVISTA

No Brasil, a utilização do BYOD ainda está amadurecendo e poucas empresas o utilizam com as devidas políticas. Com a entrevista, foi possível notar que as políticas adequadas na organização não são devidamente geradas para a utilização do BYOD e, trazem para o BYOD somente orientações a serem seguidas.

A organização entrevistada utiliza o BYOD de maneira informal, dependendo somente da conscientização de uso por parte dos colaboradores, as orientações, desde que sejam respeitadas pelos colaboradores, podem ter o efeito parecido com a implantação de políticas, porém estas não estão documentadas e não garantem que o colaborador irá segui-las fielmente.

Conforme mencionado no subcapitulo 4.2, o custo de investimento em tecnologia para assegurar as informações é alto e isso dificulta a utilização do BYOD, pois as organizações, geralmente as de pequeno e médio porte não estão dispostas a disponibilizar grande investimento, isso acontece por não ter uma equipe especializada que julgue necessário adequar-se as mudanças de tecnologia, fato mencionado na entrevista na pergunta de número dois.

Também foi possível notar que, em relação às políticas de segurança de informação, a organização entrevistada atende muitos aspectos mencionados no decorrer deste trabalho e que podem se enquadrar na utilização do BYOD, descrevendo de maneira resumida, são estes: auditoria, backup e suporte para os colaboradores.

As ações preventivas vistas no subcapitulo 2.3 são de extrema importância para que, pensando a longo prazo, auxiliem para que a organização não tenha gastos inesperados, que fugirão de seu controle de

finanças e podendo ocasionar prejuízo a mesma, requisito que em relação ao BYOD na organização entrevistada, também é tratado como orientação e não é exigido de maneira formal.

Um aspecto favorável à organização são as boas práticas estruturadas na família ISO 27000, considerando que, a ISO 27001, vista neste trabalho, no subcapitulo 2.2.2, é considerada a mais utilizada em políticas de segurança da informação, pois traz melhores padrões de proteção das informações trafegadas dento da organização, tornando-a confiável, e com isso, sendo vista com bons olhos pelos clientes.

A organização também trabalha com o bloqueio de aparelhos, não mencionando o processo para que isso ocorra, porém conforme mencionado no subcapitulo 4.2.2, este bloqueio pode ser efetuado através do MDM. Podemos notar que na organização entrevistada, também há bloqueio por acesso remoto, assim funcionalidade destaca no MDM. Podendo supor que o software de monitoramento se adéqua a requisitos parecidos com o do MDM.

Nota-se também que a organização não tem uma área especifica para gestão, tratado pelo subcapitulo 2.1 deste trabalho, porém esta trabalha com uma área especifica de segurança da informação, fator interessante que, alinhado com requisitos de gestão, pode tratar das informações com o mesmo nível de um setor especifico de gestão.

Outro aspecto relevante é o fato da organização entrevistada trabalhar com sistemas próprios e adequar advertências classificadas em níveis de violação para as políticas de segurança da informação, regrando violações ocorridas na organização, no caso do BYOD, essas advertências não podem ser utilizadas, devido ao uso deste ser através de orientações e não políticas documentadas com ligação direta ao BYOD.

A organização ainda não se voltou à conscientização de funcionários a utilização de BYOD, fator negativo para esta, uma vez que, este é um requisito primordial, pois com treinamentos de conscientização, o colaborador toma conhecimento da responsabilidade que tem sobre as informações e como a utilização indevida destas se tornam prejudiciais a organização e a ele, interferindo em suas atividades diárias, como visto no subcapitulo 2.1.

Em relação a níveis de informações e acessos, a organização entrevistada se enquadra aos requisitos de gestão, visto também no subcapitulo 2.1, aonde os acessos são disponibilizados para os colaboradores de acordo com suas necessidades e área em que exercem suas atividades.

Em análise junto ao trabalho efetuado, foi possível informar que a organização entrevistada adéqua as suas políticas de segurança da informação em relação aos conceitos estudados, porém a utilização do BYOD ainda esta sendo implantada, sendo assim, o ideal é que, os próximos passos de implantação do BYOD contenham regras documentadas, exigidas e transmitidas aos colaboradores em suas políticas.

Por fim, com a análise comparativa da entrevista junto ao estudo realizado, foram propostos aspectos que abrangem algumas áreas da organização para a implementação dessas políticas de segurança da informação voltadas para utilização do BYOD, podendo auxiliar futuramente organizações que, como a entrevistada, não dispõe de políticas de maneira documentada.

8 PROPOSTAS DE POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO PARA BYOD

Para que as políticas de segurança da Informação voltadas para BYOD sejam criadas, deve-se analisar impacto que terá no ambiente corporativo, definir responsabilidades e papeis que serão executados por cada setor para que as políticas sejam estratégicas e auxiliem o bom funcionamento das atividades diárias. (MONTEIRO, 2009, p.35)

Baseado na pesquisa bibliográfica realizada e na entrevista efetuada no estudo de caso, junto a situações corriqueiras, esse trabalho teve o intuito de propor algumas melhores práticas que poderão ser implantadas conforme necessidade de cada organização.

8.1 Divisão de responsabilidades por hierarquia

Todos dentro da organização devem colaborar para proteção de suas informações e, uma das propostas para que o objetivo de segurança seja alcançado é a divisão de deveres por área, ou seja, cada área terá suas responsabilidades.

Alta Administração:

• Analisar as políticas elaboradas; e,

• Autorizar as políticas analisadas de maneira documental.

Área de TI:

• Implementação de aplicativos autorizados nos *smartphones, tablets* e *notebook*;

• Suporte a esses dispositivos;

• Avaliação do monitoramento, que pode ser realizado através do MDM;

• Ações preventivas, detectivas e corretivas; e,
• Armazenamento dos arquivos em nuvem.

Área Jurídica ou RH:

• Revisão da documentação de políticas, antes destas serem enviadas para autorização e quando forem alteradas;
• Realização de documentos para treinamentos; e,
• Realização de termos de utilização dos dispositivos, estes são assinados pelos colaboradores.

Gestão de segurança da informação:

• Junto às informações dos setores da empresa e TI gerar políticas para utilização dos dispositivos móveis e alterá-las quando for necessário;
• Monitorar o MDM, caso seja implementado na organização;
• Enviar relatórios do MDM ao TI para avaliação do monitoramento;
• Implantar treinamentos sobre aplicativos utilizados; e,
• Implantar treinamentos sobre conscientização dos colaboradores em relação à importância das informações, utilização de dispositivos e políticas a serem seguidas.

Colaboradores:

• Trafego de informações da organização;
• Utilização dos equipamentos móveis de maneira consciente; e,
• Obedecer às políticas de segurança da informação implementadas.

8.2 Proposta de documento de dados do dispositivo móvel utilizado

O documento que indica características do aparelho utilizado pelo colaborador pode ser inserido nas políticas de segurança da informação como “documento do dispositivo móvel utilizado”, para que o gerenciamento deste seja efetuado sem problemas futuros ou empecilhos que possam ocorrer e atrapalhar no monitoramento e controle de utilização, o documento deve estabelece que o dispositivo móvel é pessoal e irá conter informações pessoais, outros requisitos que devem constar são:

• Nome do colaborador;
• Contato do colaborador (*e-mail*, número de telefone e outros meios de comunicação);
• IMEI;
• IP;
• Sistema Operacional;
• Versão;
• Modelo; e,
• Marca.

8.3 *Cheklist* de processos para BYOD

A organização pode implementar é o *checklist* de processos que descriminam exatamente o que foi solicitado dentro das políticas para cada área. Neste trabalho foi elaborado um *checklist* básico de processos voltados para organizações que trabalham com BYOD, contendo de maneira ampla, quesitos para implementação de políticas que poderão ser encaixadas em diversas áreas da organização.

Para a organização é de extrema importância o cumprimentos de requisitos para que se tenha êxito nos segmentos de políticas de segurança da informação, sendo estes importantes:

Tabela 1: Requisitos de organização

1	ORGANIZAÇÃO VISANDO COLABORADORES	ADEQUA A ORGANIZAÇÃO (S/N)
1.1	Implementar treinamentos a cada alteração de politica	
1.2	Documentar treinamentos e alterações efetuadas nas políticas de segurança da informação	
1.3	Formalizar consequências para quebra de politicas	
1.4	Disponibilizar as politicas de segurança das informações acessíveis para qualquer colaborador	
1.5	Definir como será efetuada a autenticação de usuário para cada colaborador	
1.6	Efetuar avaliação mensal junto aos colaboradores para análise de políticas exigidas, podendo alterá-las ou verificar se estão sendo seguidas	
1.7	Definir tratamento para perda de dispositivo móvel junto ao TI	
1.8	Caso a gestão da informação seja efetuada direto pelo colaborador, deve-se documenta-la	

1.9	Efetuar prova documental de regras e normas, assinada pelo gestor, diretor e colaborador	

Fonte: Autoria própria

Para a área de TI, cabe analisar melhores diretrizes de ações que irão impulsionar a utilização do BYOD de maneira adequada, sendo estas:

Tabela 2: Requisitos de TI

2	TI	ADEQUA A ORGANIZAÇÃO (S/N)
2.1	Definir como será efetuado o suporte aos dispositivos móveis e qual horário que este estará disponível	
2.2	Disponibilizar acesso à *Internet* para utilização do BYOD	
2.3	Auditar os dispositivos móveis periodicamente	
2.4	Efetuar cópias de segurança periódicas	
2.5	Realizar ação preventiva de verificação mensal dos dispositivos móveis	
2.6	Analisar a melhor utilização dos sistemas da organização nos dispositivos móveis	
2.7	Analisar quais os aspectos mais relevantes para utilização de BYOD, auxiliando a gestão na geração de políticas	
2.8	Definir aplicativo do sistema da organização para utilização no dispositivo móvel	
2.9	Definir ações preventivas, detectivas e corretivas de maneira periódica	

Com a análise do BYOD, efetuada pelo TI é necessário seguir critérios para sua utilização

Tabela 3: Requisitos de utilização

3	UTILIZAÇÃO DO BYOD, CLOUD COMPUTING E GERENCIAMENTO DE MONITORAÇÃO	ADEQUA A ORGANIZAÇÃO (S/N)
3.1	Monitoramento de utilização dos dispositivos móveis	
3.2	Utilizar o gerenciamento de dispositivos móveis	
3.3	Analisar sistemas operacionais utilizados que sofrem constantes atualizações	
3.4	Monitorar arquivos utilizados em nuvem	
3.5	Bloquear dispositivos em caso de perda ou furto	
3.6	Definir lista de aplicativos que não podem ser utilizados nos dispositivos móveis	
3.7	Controlar o desempenho dos colaboradores com utilização do BYOD, para medir a viabilidade de sua utilização	
3.8	Gerar relatórios de monitoramento do gerenciamento de dispositivos	

Na área de gestão, o objetivo é garantir que a utilização positiva do BYOD seja regrada e documentada, para isso é necessário que os requisitos voltados aos controles e monitorias sejam praticados, encaminhados então para análise pelo TI.

Os requisitos essenciais que devem ser verificados para uma boa gestão de segurança da informação são:

Tabela 4: Requisitos de Segurança da Informação

4	GESTÃO DE SEGURANÇA DA INFORMAÇÃO	ADEQUA A ORGANIZAÇÃO (S/N)
4.1	Efetuar controles de acessos, transmissões e recebimento de informações periodicamente	
4.2	Definir tratamentos para violações de das políticas de segurança da informação	
4.3	Enquadrar políticas de boas práticas baseadas no ITIL E ISO 27001	
4.4	Implementar níveis de proteção as informações	
4.5	Documentar liberações de acessos	
4.6	Avaliar os níveis de criticidade das informações trafegadas nos dispositivos móveis	
4.7	Avaliar os níveis de criticidade das informações trafegadas	
4.8	Definir controles de riscos e ameaças que surgem com a utilização dos dispositivos móveis	

4.9	Definir tratamentos para perda ou furto dos dispositivos móveis pessoais	

9 CONSIDERAÇÕES FINAIS

Foi possível concluir que o fenômeno BYOD tem tomado grande força desde sua criação até o presente momento, sendo visto com bons olhos pelas organizações com grande fluxo de informações, porém o BYOD é utilizado por empresas de grande porte e no Brasil, ainda não ganhou a devida notoriedade pelas corporações.

Pode se identificar também que para adequar o fenômeno BYOD, as organizações devem aderir a políticas de segurança da informação, estas devem ser documentadas. Torna-se necessário à implementação da gestão de segurança da informação, pois por se tratarem de dispositivos pessoais, o risco de vulnerabilidades obtidas torna-se maior.

Os dispositivos móveis devem ser auditados e gerenciados periodicamente com ações preventivas para que haja controle de aplicativos mais acessados, quais os riscos que eles podem trazer com as informações são acessados, transmitidas e recebidas.

Com o estudo sobre o BYOD, foi possível abranger melhor a área de políticas de segurança da informação, uma vez que o BYOD tem ligado a ele outras ferramentas que são de grande utilidade para as organizações, como o MDM para gerenciamento dos dispositivos e o *Cloud Computing*, proporcionando outro meio de arquivo de informações, de maneira simples e de fácil utilização.

Vale ressaltar que com o estudo, foi possível adentrar a critérios que devem ser exigidos em uma organização para que suas informações estejam sempre asseguradas, tanto para o BYOD, como para processos utilizados em equipamentos fixos e processos que já haviam sido impostos nas atividades exercidas.

No Brasil, existem poucos profissionais com vasta experiência sobre o assunto, fazendo com que o crescimento do BYOD ainda seja demorado não haja muito conhecimento sobre o assunto pela maioria das pessoas.

O principal problema identificado foi que a falta de políticas de segurança da informação nas organizações podendo vir a causar problemas futuros em grandes proporções. Ainda são poucas as organizações que trabalham com recursos de segurança com prioridade e de maneira preventiva, principalmente as de pequeno porte, estas raramente controlam o uso dos dispositivos móveis de seus colaborados, deixando-os vulnerável a ataques maliciosos.

A organização abrangerá claramente os riscos e vulnerabilidades que possam vir a ser atacados caso a informação de perca, para que os colaboradores saibam a maneira correta de utilizar e transmitir informações em suas atividades diárias e devem ser documentadas e arquivadas, para caso sejam necessárias no futuro.

No entanto há políticas de segurança da Informação que já são aplicadas em empresas, sem que haja documentação sobre a mesma, com uso inconsciente, porém é necessário preparo para que políticas sejam aplicadas e exigidas de seus colaboradores. Há necessidade também de gestão para a segurança da informação, onde especialistas conseguem controlar todos os recursos utilizados dentro da organização e podem impor a utilização de políticas de segurança da informação.

A análise de políticas de segurança da informação, BYOD e gestão trouxeram exemplos de experiências vivenciadas com atividades, processos e políticas que já haviam sido exercidas de maneira inconsciente. Com isso, foi possível visualizar falhas e implementações que podem ser revistas e analisadas, algumas destas experiências foram relacionadas a materiais neste trabalho.

Como continuidade deste trabalho, é possível abordar um estudo com embasamento em documentação de políticas de segurança da informação e documentação especifica para políticas de segurança da informação para BYOD, para analise e implantação de modelos e requisitos necessários para a geração destes documentos. Sendo possível alinhar ao contrato de trabalho, as especificações das políticas e de maneira judicial, para que essas políticas possam ser exigidas dos colaboradores.

Por fim, foi possível identificar a grande dificuldade na obtenção de informações exatas sobre o fenômeno BYOD, uma vez que, os materiais para embasamento e propostas de políticas de segurança da informação voltadas para o BYOD são escassos e em sua grande maioria, em outro idioma. Para obtenção de informações sobre como é, qual utilidade e ou aspectos do BYOD foram necessários acessos a páginas especificas sobre o assunto, blogs somente para a visualização de referencias em comparação de informações obtidas nas páginas diretas ao assunto, traduzidas de artigos estrangeiros.

REFERÊNCIAS

ABNT. Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27001: 2006**: tecnologia da informação – técnicas de segurança. Rio de Janeiro: ABNT, 2011.

ABNT. Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27001: 2013**: tecnologia da informação – técnicas de segurança. Rio de Janeiro: ABNT, 2013.

ALECRIM, Emerson. **O que é cloud computing**? São Paulo: Infowester, 2008. Disponível em <http://www.infowester.com/cloudcomputing.php> Acesso em: 23 set. 2015. 16h05m.

ALMEIDA, Everton. **Sistema de Gestão de Segurança da Informação** (SGSI) – Parte I Disponível em: <http://www.tiespecialistas.com.br/2013/10/sistema-gestao-seguranca-informacao-sgsi-i/> Acesso em 06 out. 2015. 13h59m

AMOROSO, Danilo. **O que é computação em nuvens**? São Paulo: Tecmundo, 2012. Disponível em: <http://www.tecmundo.com.br/computacao-em-nuvem/738-o-que-e-computacao-em-nuvens-.htm> Acesso em: 29 set. 2015. 18h12m

CASTRO, Iury Martins; SOUZA, Samuel Camargo. **Consumerização de TI**: solução Open-Source para gerenciamento de dispositivos móveis em organizações que utilizam BYOD. Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação, Três de Maio, v.1, n.3, 2015 Disponível em: http://revistas.setrem.com.br/index.php/reabtic/article/view/103. Acesso em 30 set. 2015. 17h33m.

COCCHI, Debora. **Política de segurança da informação para aplicação BYOD**. Disponível em: <http://www.profissionaisti.com.br/2013/06/politica-de-seguranca-para-aplicacao-byod/> Acesso em 25 set. 2015. 14h21m.

CUNHA, I. K. B. ; CASTRO, R. C. C. . **Gestão de segurança da informação em ambiente BYOD**: um mecanismo de apoio baseado nas boas práticas ITIL. In: Encontro Anual de Tecnologia da Informação - EATI, 5, 2014, Frederico Westphalen. Trabalhos apresentados no V EATI, 2014. v. 4. p. 32-39. Disponível em: <http://www.eati.info/eati/2014/assets/anais/artigo3.pdf > Acesso em 28 set. 2015. 14h12m.

DAWEL, George. **Segurança da informação nas empresas**: ampliando horizontes além da tecnologia. Rio de Janeiro: Ciência Moderna, 2005.

DODT, Claudio. Disponível em: **Consumerização, BYOD e MDM**: indo além da sopa de letrinhas da mobilidade. Disponível em < http://claudiododt.com/pt/tag/consumerizacao/> Acesso em 16 nov. 2015. 13h46m

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

FONTES, Edison, CISM, CISA. **Políticas e normas para a segurança da informação**: como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações. Rio de Janeiro: Brasport, 2012.

FONTES, Edison, CISM, CISA. **Praticando segurança da informação**. Rio de Janeiro: Brasport, 2008.

FONTES, Edison, CISM, CISA. **Segurança da informação**: o usuário faz diferença. São Paulo: Saraiva, 2006.

GIORGI, Ricardo. **Segurança em dispositivos móveis**. Disponível em: <https://www.fiap.com.br/2014/10/13/fiapx/seguranca-em-dispositivos-moveis/> Acesso em: 29 set. 2015. 22h49m

MANSUR, Ricardo. **O que é ITIL**? São Paulo: TrendBiz, 2009. Disponível em: <http://www.profissionaisdetecnologia.com.br/blog/?p=168> Acesso em: 28 set. 2015. 16h16m.

MARSHALL, Sarah. IT Consumerization: a case study of BYOD in a healthcare setting. **Technology Innovation Management Review,** Otawa, march 2014. Disponível em:

http://timreview.ca/sites/default/files/Issue_PDF/TIMReview_March2014.pdf Acesso em: 01 set. 2015. 11h01m

MONTEIRO, Iná Lucia Cipriano De Oliveira. **Proposta de um guia para elaboração de politicas de segurança da informação e comunicações em órgãos de administração pública federal**. 2009, 67f. Monografia (Especialização em Gestão da Segurança da Informação e Comunicações) – Instituto de Ciências Exatas. Departamento de Ciência da Computação, Universidade de Brasília, Brasília, 2009. Disponível em: http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/ina_lucia.pdf. Acesso em: 29 out. 2015. 23h59m

MORETTI, João. **BYOD**: como as empresas devem avaliar e se precaver. Disponível em: <http://www.tiespecialistas.com.br/2013/02/byod-como-as-empresas-devem-avaliar-e-se-precaver/ > Acesso em: 23 set. 2015. 16h33m.

MORETTI, João. **MDM**: A solução ideal para gerenciar os dados nos dispositivos móveis corporativos. Disponível em: <http://imasters.com.br/infra/seguranca/mdm-a-solucao-ideal-para-gerenciar-os-dados-nos-dispositivos-moveis-corporativos/> Acesso em: 23 set. 2015. 17h18m.

MOSENA, Aline. **Itil, e agora**? Disponível em: <http://www.tiespecialistas.com.br/2015/08/itil-e-agora/> Acesso em: 28 set. 2015. 15h53m.

MUNDO-ITIL. **O que é ITIL**? Disponível em: <http://www.mundoitil.com.br/certificacao-itil/> Acesso em: 28 set. 2015. 17h01m

MUNIZ JUNIOR, Rodrigo Ramiro. **Desafios de BYOD em redes emergentes**. 2013. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/2522/1/CT_GESER_III_2013_07.pdf> Acesso em: 24 set. 2015. 12h22m

OLHAR DIGITAL. **Programa de variedades**. São José dos Campos: Lumiar, 2005-presente. Exibição: Emissora de televisão original: Rede TV (2005-13) PlayTV (2005-?) Sony, AXN (2013-presente).

PESSOA, Cristiano Alves. **O que é BYOD**. São Paulo: Oficinadanet, 2013. Disponível em: <https://www.oficinadanet.com.br/post/11708-o-que-e-byod> Acesso em: 29 set. 2015. 17:37m

REZENDE, Denis Alcides. **A evolução da tecnologia da informação nos últimos 45 anos.** Joinville: UDESC, 2011. Disponível em: http://www.joinville.udesc.br/portal/professores/pfitscher/materiais/Evolu__o_da_TI.pdf. Acesso em 26 out. 2015 18h33m

RHEE, Keunwoo; JEON, Woongryul; WON, Dongho. Security Requirements of a Mobile Device**. International Journal of security and its applicationsManagement System,** Tasmânia, v.6, n.2, April, 2012 Disponível em: <http://www.sersc.org/journals/IJSIA/vol6_no2_2012/49.pdf> Acesso em 30 out. 2015 19h15m

SANTOS, F. N. ; FRESCHI, J. C. **A evolução da TI e os impactos na administração das empresas**. **Revista Terceiro Setor**, Guarulhos, v.78, n.1, 2013. Disponível em: http://revistas.ung.br/index.php/3setor/article/viewFile/1907/1502. Acesso em 04/01/2016

SHIBATA, Luís Minoru et al. **BYOD**: como preparar seus negócios para uma avalanche de dispositivos. São Paulo: PromonLogicalis, 2012. Disponível em: <http://www.br.promonlogicalis.com/globalassets/latin-america/advisors/pt/advisor-byod.pdf> Acesso em: 17 nov. 2015. 01h17m.

SILVA, Passos Vinicius. **Você sabe o que significa consumerização? está preparado para ela**? Disponível em: <http://www.tiespecialistas.com.br/2012/04/voce-sabe-o-que-significa-consumerizacao-esta-preparado-para-ela/> Acesso em 06 out. 2015 23h35m

SILVA NETTO, Abner da. **Gestão de segurança da informação**: fatores que influenciam sua adoção em pequenas e médias empresas. 2007, 107f. Dissertação (Mestrado em Administração) – Universidade Municipal de São Caetano do Sul, São Caetano do Sul, 2007 Disponível em:

http://www.uscs.edu.br/posstricto/administracao/dissertacoes/2007/abner_da_silva_neto/dissertacao_AbnerNetto.pdf. Acesso em: 21 set. 2015. 10h14m.

SLIDE **Share**. Disponível em: <http://pt.slideshare.net/suelybcs/tira-dvidas-sobre-skydrive-google-drive-e-dropbox-afinal-qual-usar> Acesso em: 28 out. 2015. 17h25m

SPICE Works. Disponível em: <http://www.spiceworks.com/free-mobile-device-management-mdm-software> Acesso em: 29 out. 2015. 02h50m

STAGLIANO, Thomas; DIPAOLO, Anthony; COONELLY, Patricia. The consumerization of information technology. **Graduate Annual**, Philadelphia, v.1, Article 10, 2013.. Disponível em : <http://digitalcommons.lasalle.edu/graduateannual/vol1/iss1/10> Acesso em: 11 nov. 2015. 01h12m

TAURION, Cezar. **A vez do BYOC** (Bring Your Own Cloud). Disponível em: < http://www.tiespecialistas.com.br/2012/10/a-vez-do-byoc-bring-your-own-cloud/#.UaYU1tiMH3V> Acesso em: 23 set. 2015. 17h48m.

TELECO-WORLD. **Estatísticas de celular no mundo**. Disponível em <http://www.teleco.com.br/pais/celular.asp> Acesso em: 23 set. 2015. 16h15m.

WAZLAWICK, Raul Sidnei. **Metodologia de pesquisa para ciência da computação**. Rio de Janeiro: Elsevier, 2009

APÊNDICE A - QUESTIONÁRIO DE ENTREVISTA - Questionário de perguntas e respostas sobre políticas de segurança da informação implantadas da organização “X” com aspectos em BYOD. Entrevista concedida pelo professor Edson Roberto Gaseta em 29 de outubro de 2015.

1ª - Há políticas BYOD especificas na organização aonde você trabalha? Se sim, quais são as elas?
Resp.: Não existe uma política formada para o uso de BYOD. O que existe são orientações de como utilizar o seu próprio equipamento dentro e fora da empresa.
2ª - Quais foram às maiores dificuldades e pontos críticos na implementação do BYOD? E as maiores facilidades?
Resp.: Como não foi implantado oficialmente, as maiores dificuldades identificadas para a implantação foram em não permitir que aplicativos instalados nos equipamentos próprios não interferissem nas aplicações da empresa. Os pontos mais críticos estão nos aplicativos e políticas que devem auditar, monitorar e garantir que ações indevidas não estão sendo praticadas. O investimento em aplicações deste tipo é caro e o custo de customização e operação são altos, por isso não são integralmente implantadas o BYOD. Sem gestão adequada não é garantida a segurança efetiva das informações da empresa.
3ª - Há uma gestão de riscos para BYOD? Se sim, há um gestor?
Resp.: Foi feito uma análise dos riscos para a implantação, liderada pela equipe de segurança da informação da empresa, porém não foi definido nenhum gestor.
4ª - Como são tratados os casos de violações das políticas de segurança impostas na organização?
Resp.: Basicamente em 3 níveis, dependendo da gravidade da violação é feita uma categorização, que pode gerar as seguintes ações:
• Advertência leve (com registro no RH) com capacitação na política;
• Advertência formal (com registro no RH) com capacitação na política e orientação as infrações, alertando para que não ocorra mais;
• Advertência formal, com suspensão ou demissão.
5ª - Quais são as principais medidas adotadas para treinamento dos colaboradores referente à utilização do BYOD e qual a frequência de treinamentos?
Resp.: Ainda não foram realizadas ações formais para este assunto.
6ª - Como é avaliado o nível de criticidade de cada informação?
Resp.: É utilizada a classificação da informação e configurado as permissões de acesso de acordo com o perfil do funcionário e as atividades que ele realiza.
7ª - A organização trabalha com sistema próprio? Este pode ser utilizado nos dispositivos móveis de qual maneira?
Resp.: Vários sistemas próprios podem ser utilizados de dispositivos móveis de acordo com o perfil do funcionário e sempre com a utilização de VPN ou conexão segura (HTTPS).
8ª - Como é feito e controlado o monitoramento do trafego de informações transmitidas e recebidas pelos colaboradores no dia a dia?
Informação não liberada pela organização.
9ª - Já houve furto de informações na organização? Quais são os maiores riscos e vulnerabilidades dos dispositivos móveis?
Informação não liberada pela organização.
10ª - Como é tratada a perda de um dispositivo móvel?

Resp.: Todos os dispositivos móveis da empresa possuem seguro contra roubo e o bloqueio para acesso remoto é feito assim que a área de TI recebe o comunicado da perda.
11ª - Existem ações preventivas para o uso do BYOD?
Resp.: Apenas orientações em relação ao uso.
12ª - São efetuadas cópias de segurança dos dados obtidos nos dispositivos móveis? Se sim, como são efetuadas?
Resp.: São efetuadas backups por configuração de política automatizada.
13ª - Há alguma política de utilização que utilize a ISO 27001 referente a boas práticas dos colaboradores?
Resp.: Todas as políticas de segurança da empresa são baseadas na família ISO 27000 e demais boas práticas internacionais de segurança da informação.
14ª - Como é efetuado o suporte dos dispositivos móveis utilizados pelos colaboradores e em que horário é disponibilizado?
Resp.: Pela equipe de TI no horário de trabalho, das 8h00 as 17h00.

Mariana Beltran Cometti
Graduanda em Tecnologia da Segurança da Informação pela Faculdade de Tecnologia de Americana. Atualmente trabalha na área comercial com softwares de gestão empresarial pela Sage Brasil Software. Anteriormente foi suporte de TI na, atendendo clientes, implantando e testando sistemas de gestão pela Prodata Evolução em Sistemas, desligando se em novembro/2015.
Contato: mariana.cometti@gmail.com
Fonte: CNPQ – Curriculo Lates

Alexandre Garcia Aguado
Mestre em Tecnologia e Inovação pela Faculdade de Tecnologia da Unicamp (2012) e Graduado em Tecnologia em Software Livre pelo Centro Universitário Salesiano de São Paulo (2007). Atualmente é professor no Instituto Federal de São Paulo - Campus Capivari, onde coordena o Projeto Jovem Hacker - Capivari. Antes de iniciar a carreira acadêmica foi Analista de Sistemas na Celestica Corporation, suportando os sites do Canadá, EUA, México e Brasil, desligando-se em Setembro/2009. Durante todo o ano de 2011 esteve em Angola como Voluntário através dos Salesianos de Dom Bosco onde coordenou as atividades de estruturação da área de Tecnologia da Informação, tendo como foco a criação de infraestruturas de T.I das obras Salesianas e estruturação dos programas de Formação Profissional em Informática de Jovens Angolanos.
Contato: ale.garcia.aguado@gmail.com
Fonte: CNPQ – Curriculo Lates

Justificativa
O tema partiu de uma aula do sexto semestre, onde este foi visto de maneira detalhada e especifica. O BYOD - Bring Your Oun Device, ou traga seu próprio dispositivo, trabalha com a utilização de dispositivos móveis em ambientes corporativos. O tema é muito trabalhado hoje no Brasil, porém de maneira inconsciente e sem nomeação, sem políticas especificas, tornando sua utilização vulnerável.