BYOD: PRÁTICAS DE GESTÂO DE SEGURANÇA DA INFORMAÇÂO PARA DISPOSITIVOS MOBILE EM AMBIENTES ACADÊMICOS NO MODELO 'BRING YOUR OWN DEVICE'

Melky Fanti Dueñas

Resumo: Este trabalho de pesquisa está focado em políticas de segurança da informação para o uso de dispositivos mobile em instituições de ensino. São explanados conceitos da segurança da informação, técnicas de gestão de segurança da informação e é apresentado uma nova realidade praticada nos dias atuais em organizações e instituições: O uso do Bring Your Own Device(BYOD). Ao final é feita uma reflexão das necessidades das instituições de ensino comparadas com as necessidades de organizações de outras áreas e abre-se um nicho para possíveis trabalhos voltados para instituições acadêmicas onde um maior sigilo de suas informações é exigido.

Palavras-chave: Segurança. Gestão. BYOD. Mobile . WIFI.

1 INTRODUÇÃO

As redes *WIFI*, antes consideradas um serviço incremental em instituições, hoje já são um serviço essencial em várias instituições e organizações de várias vertentes. Muitos setores não podem mais se imaginar sem conexão sem fio para realizar suas tarefas do dia-a-dia, obrigando as instituições a investir cada vez mais em um serviço de rede sem fio cada vez mais completo e eficiente.

A princípio as instituições projetavam suas redes sem fio para uso exclusivo de seus próprios dispositivos, em geral *desktops*, os quais eram totalmente configurados e gerenciados internamente, a TI possuía total controle do que era instalado, das permissões e restrições de acesso e em geral o usuário do dispositivo não podia alterar nenhuma regra desse ambiente mas, com o avanço da tecnologia *mobile* e a redução significativa nos custos de *tablets* e *smatphones e notebooks*, a utilização desses dispositivos em redes de instituições teve grande crescimento.

Onde antes dúvidas eram tiradas somente em livros didáticos, na biblioteca da instituição ou em seus laboratórios de informática, alunos e professores agora tem celulares, *tablets* e *notebooks* que podem rapidamente sanar dúvidas e/ou buscar por conteúdos complementares à aula com uma simples busca na *Internet*, professores podem baixar e postar material de aula nos servidores, fazer chamada *on-line* e até utilizar *sites* de mídia para enriquecer suas aulas. Instituições acadêmicas muitas vezes realizam cursos e palestras em suas dependências e os palestrantes em geral utilizam seus *notebooks* para ministrar o conteúdo. Não ter um ambiente adequado com conexão rápida e fácil para o

visitante pode gerar complicações no evento a ser realizado como atraso ou até prejuízo de seu conteúdo, sem considerar que a imagem da TI da instituição pode ficar prejudicada. Outra demanda pode ser a necessidade um professor ou aluno necessitar conectar seu *notebook* à rede cabeada, seja para uma aula específica ou a transferência de um arquivo contendo vários *Gigabytes*, como garantir essa conexão específica sem comprometer a segurança da informação?

A Gestão de segurança da informação nessas instituições, se limitava a gerenciar seu parque de equipamentos, e apenas isolar a rede *WIFI* quando existente, oferecendo apenas acesso à I*nternet* para *notebooks* dos usuários, muitas vezes fazendo seu acesso por meio de *Access Points* domésticos e com um método de autenticação considerado fraco, com um usuário e senha compartilhado para todos os usuários. Com o crescimento do fenômeno BYOD nessas instituições, esse ambiente demanda por mudanças na gestão de segurança da informação visto que agora alunos e professores possuem *smartphones, tablets e notebooks* capazes de realizar todas as suas tarefas, fazendo com que a administração do ambiente aceite o uso de tais dispositivos sem abrir mão da segurança de seus ativos.

Esse estudo teve o objetivo de encontrar melhores práticas para a Gestão de Segurança da Informação realizada nessas instituições de ensino considerando o BYOD se utilizando de métodos e técnicas já existentes ou as adaptando para que melhor se adequem ao ambiente acadêmico.

Primeiramente são tratados os elementos para realizar a Gestão de Segurança da Informação e como ela é realizada atualmente na maioria das instituições, também são tratados alguns conceitos de computação mobile, suas vantagens e os riscos que surgem com o seu uso.

Em seguida são apresentados os resultados obtidos na pesquisa, que são, de acordo com o material pesquisado, práticas que melhor se enquadram para a Gestão de Segurança em um ambiente BYOD nas instituições de ensino. Quais são os métodos e tecnologias, e como devem ser utilizados pela equipe de TI da instituição.

Para a realização da pesquisa foi utilizada literatura bibliográfica voltada para a Gestão de Segurança da Informação, contemplando desde a parte gerencial/operacional até a parte de tecnologia específica, estudando normas já bem difundidas no mercado e livros que tratam do assunto pesquisado.

Para finalizar o estudo abre espaço para as conclusões tiradas durante a pesquisa, quais as melhores práticas encontradas para o ambiente proposto, se foi necessário a criação de práticas específicas e/ou foram encontradas práticas já existentes que atendem aos requisitos de um ambiente acadêmico utilizando BYOD.

2 A BASE DE ESTUDO

2.1- A informação

Nos dias atuais a informação é o bem mais precioso que uma organização possui. Garantir que a informação esteja devidamente protegida é fundamental para sua sobrevivência.

Segundo Fontes (2006), "A informação, independente de seu formato, é um ativo importante da organização".

A Segurança da Informação deve ser gerida pela organização sempre visando garantir suas principais propriedades.

De acordo com (FERREIRA; ARAUJO, 2008) as propriedades são:

- **Confidencialidade**: é a garantia de que a informação só será acessada por pessoas com a autorização necessária. A não conformidade com essa propriedade pode acarretar em acesso não autorizado, alteração e até roubo de informação.
- **Disponibilidade**: é a garantia de que a informação estará sempre disponível para as pessoas que a requisitar. A não conformidade pode gerar parada parcial ou total de serviços essenciais para a sobrevivência da organização.
- **Autenticidade**: é a garantia de que a informação recebida foi enviada pelo real remetente da mesma. A não conformidade desta propriedade pode gerar vulnerabilidades para ataques baseados em spoofing e man in middle.

2.2- A Gestão de Segurança da Informação

Sabendo que a informação é o bem mais precioso de uma organização, manter ela protegida é de extrema importância. Nos dias atuais ocorrem casos de ataques e roubos de informações e invasões por meios eletrônicos. (FONTES, 2008)

Uma organização que possua um SGSI (Sistema de Gestão de Segurança da Informação) pode garantir maior segurança de suas informações.

Um SGSI efetivo deve contar com um setor de TI dedicado, com profissionais capacitados, uma política de gestão e segurança bem definida e implantada, funções e responsabilidades bem claras e um gestor competente. O gestor precisa ser um

profissional que tenha a visão e entendimento de toda a organização e das atividades realizadas nela.

Tendo a pessoa dedicada à segurança da informação um conhecimento vasto, a criação e implantação de políticas se torna mais específica. (FONTES, 2008)

2.3- A Computação Mobile e a Consumerização

Cada vez mais, usuários possuem seus próprios dispositivos que são capazes de realizar todas as tarefas realizadas antes pelos equipamentos das instituições. O uso de computadores *desktop* vem caindo nos últimos anos, e na contra-mão o uso de dispositivos *mobile* vem crescendo, esse fato é conhecido como a consumerização da TI.

Segundo (DODT, 2013), a "consumerização é a tendência de que tecnologias desenvolvidas com foco no mercado consumidor adentrem a esfera corporativa."

A consumerização se deve ao grande crescimento do mercado de consumo, em que os fabricantes de produtos eletrônicos se viram obrigados a produzir aparelhos para uso residencial e disponibilizá-los em um valor menor que os aparelhos de uso comercial.

Para (GARANHANI ,2013), a consumerização "ajuda a desenvolver dispositivos com plataformas de aplicativos mais inteligentes e serviços personalizados", como por exemplo a *cloud computing* e o uso de redes sociais.

Levando em consideração as afirmações dos autores citados acima, seria natural esperar que era questão de tempo até que os usuários de aparelhos *mobile* (celulares, *tablets*, *notebooks*) por usar esses aparelhos em um nível tão profundo para fins pessoais, desejariam usá-los também para fins profissionais e acadêmicos , conectando se às empresas e faculdades onde frequentam para realizar suas tarefas. Essa tendência ficou conhecida como BYOD (Bring Your Own Device).

2.4- BYOD

O fenômeno causado pela consumerização de dispositivos *mobile*, onde as pessoas passaram a usar seus dispositivos particulares para fins profissionais, além de fins pessoais, ficou conhecido como BYOD (Bring Your Own Device).

Para grande número de empresas, principalmente na Ásia e América Latina, o BYOD é visto com bons olhos, visto que aumenta a produtividade e satisfação dos colaboradores e reduz o custo com aquisição de equipamentos. (Cisco IBSG, 2012)

As vantagens do BYOD são inúmeras, desde trabalhar com seus *softwares* e apps favoritos até poder trabalhar de qualquer lugar com uma conexão de *Internet*, acessando

os recursos da empresa por uma VPN por exemplo. Mas a maior vantagem é a satisfação dos funcionários. (KEYES, Jessica, 2013)

Entre as desvantagens a segurança é unanimidade.

O uso de dispositivos *mobile* vem crescendo exponencialmente, mas a efetividade na segurança desses dispositivos não tem acompanhado a demanda. Segundo (KEYES, Jessica, 2013) 4% dos *smatphones* são roubados ou perdidos a cada ano e esses aparelhos roubados podem abrir uma brecha de segurança, expondo dados sensíveis da organização.

2.5- A Segurança Mobile

A segurança da informação para *mobile* se faz diferente de uma segurança de informação tradicional, contendo *desktops* e *notebooks*.

De acordo com (Souppaya e Scarfone, 2013) alguns dos principais fatores que colaboram para a falta de segurança no ambiente *mobile* são:

- **Falta de segurança física** – Os dispositivos podem ser usados em vários lugares, seja em cafés, aeroportos, hotéis, e até mesmo em vários lugares dentro da própria organização. Isso facilita furtos e roubos, expondo as informações se não houver uma mitigação correta do risco.

- **Uso de dispositivos e redes não confiáveis** – O uso de dispositivos *mobile*, principalmente aqueles de uso pessoal dos funcionários (BYOD), não oferecem a segurança para os ambientes corporativos e/ou acadêmicos. Jailbreak são constantemente realizados, permitindo *by-pass* das restrições de segurança do sistema operacional.

Também há o uso de redes não confiáveis, o que aumenta o risco de ataques *man-in- middle* e pode até interceptar e modificar as comunicações.

- **Interação com outros sistemas** - Os dispositivos *mobile* podem ser conectados à outros dispositivos (*desktops, notebooks*) para vários fins, seja para carregar a bateria, compartilhar conexão de internet, sincronizar arquivos. Essa ação abre brechas permitindo possíveis ataques à rede da instituição através do computador ao qual o dispositivo está conectado.

3 AS BOAS PRÁTICAS PARA GESTÃO DE SEGURANÇA EM AMBIENTES BYOD

A seguir são apresentados os resultados da pesquisa realizada:

3.1- Politica de segurança da informação - Para a adoção de boas práticas em qualquer ambiente tecnológico em uma instituição, a primeira coisa a ser feita é a criação e adoção e uma política de segurança da informação. Essa política deve ser elaborada pelos responsáveis de TI junto à administração da instituição e implantada pela equipe de TI. Deve ser divulgada para conhecimento e seguida por todos os stakeholders da instituição.

3.2- Politica de uso do ambiente mobile- Essa politica deve ser elaborada pelos gestores de TI, contento todas as regras para uso do ambiente *mobile*. Nela devem conter tudo oque se pode e não ser feito, acessado, executado dentro do ambiente e as implicações em caso de alguma violação. De acordo com a ISO/IEC27002, convém que a política considere dentre outros requisitios:

- Registro dos dispositivos móveis;
- Restrição para conexão aos serviços de informação;
- Controle de acesso;
- Técnicas criptográficas;
- Desativação, bloqueio e exclusão de forma remota;

3.3- Termo de aceite de uso do ambiente mobile- Esse termo deve conter todas as regras da Politica do item anterior e deve ser apresentado para o usuário antes que ele comece a usar o ambiente mobile onde ele pode concordar com todos os termos e esse ‘aceite’ ficar registrado e armamazenado pela administração do serviço. Esse termo pode ser apresentado ao fututo usuário em papel e/ou armazenado em arquivos ou digitalmente. Um endereço web pode ser disponibilizado e ser acessado por um equipamento da instituição(Ex: computador de laboratório) ou pelo próprio dispositivo do usuário em seu primeiro acesso, nesse endereço é apresentado toda a Política de uso do serviço e o 'Submit' de aceite ou não. Em caso de aceite, essa submissão deve ser vinculada à credencial de usuário e devidamente armazenada.

3.4- Plano de tratamento de incidente - Um plano de tratamento de incidentes deve ser elaborado pela equipe de TI. Em caso de os controles de segurança falharem e algum dispositivo mobile causar algum incidente de segurança, procedimentos e técnicas devem ser estabelecidas para a contenção e extinção dos mesmos. Esse plano deve conter recursos que permitam a administração do serviço monitorar e excluir dispositivos e usuário potencialmente perigosos.

3.5- Acesso Lógico

- ***Mobile*** **-** O acesso à rede mobile aos recursos da instituição deve ser feito de forma segura, garantindo a integridade e confidencialidade das informações manipuladas. Não só uma boa prática, mas um método essencial para garantir a segurança da informação é implantar um método de autenticação, permitindo somente usuários autorizados. Essa autenticação pode ser feita de várias formas, pelo próprio *Access Point* ou por um servidor de autenticação em conjunto com o *Access Point*.
- **Cabeado -** Os dispositivos que acessam a rede por cabeamento devem passar por identificação e autenticação da mesma forma que os dispositivos *mobile.* Todos os pontos de rede devem ter seu acesso bloqueado, permitindo somente dispositivos autorizados a se conectar por meio de autorização e autenticação, isso impede que dispositivos BYOD não autorizados se conectem a rede cabeada, que pode possuir politicas de acesso diferentes do ambiente *mobile*, também impede técnicas como *sniffing* nessas subredes e o uso de *rogue APs.* Em caso de necessidade de acesso à rede cabeada por um dispositivo BYOD, as politicas de uso devem estar definidas na 'Politica de uso do ambiente mobile', e a autorização deve ser avaliada pela administração levando em consideração as seguites questões:
    - Qual o propósito do uso da rede cabeada ?
    - O propósito justifica os riscos envolvidos ?
- **Acesso Externo -** O acesso externo, quando necessário, deve ocorrer por meio de uma conexão segura com a instituição. Recomenda-se o uso de uma VPN(*Virtual Private Network*) para esse fim. Uma VPN permite

conexão por meio de um túnel criptografado com a instituição de maneira simples e segura utilizando a Internet. É recomendável que a conexão seja feita por meio de autenticação e com uso de certificados digitais gerados pela instituição. É importante que a administração tenha registrado todos os usuários e dispositivos que terão permissão para realizar acesso externo assim como manter registros de log das atividades realizadas.

3.6- Acesso Físico

Assim como o acesso lógico, o acesso físico ás instalações da instituição também deve ser controlado. O acesso de pessoas não autorizadas a locais e de acesso restrito pode gerar perda, roubo e alteração de dados. A ISO/IEC 27001 destaca entre outros alguns métodos para controle de acesso físico que se aplica a instituições de ensino como:

- **Perímetro de segurança física** - deve ser definido esse perímetro para proteger as áreas de instalações de processamento de dados e informações sensíveis. Uma recepção com métodos de acesso pode ser implantada, garantindo que somente alunos, professores e outras pessoas autorizadas acesse as dependências da instituição;
- **Controles de entrada física** - As áreas seguras devem ser protegidas por controles apropriados para garantir que somente pessoas apropriadas tenham acesso ao perímetro. Convém que a data e hora em que as pessoas acessam o perímetro sejam registradas. Visitantes devem ser supervisionados, salvo casos em que seu acesso tenha sido previamente aprovado;

3.7- Identificação e Autenticação – Todo usuário autorizado a utilizar a rede da instituição deve possuir um ID de acesso (Nome de usuário) que seja único entre todos os IDs de usuários da rede. Segundo a ISO/IEC 27033-1, um *secure single sign-on* (SSO) pode reduzir o número de informação de autenticação que os usuários são solicitados a proteger, aumentando dessa forma a eficácia desse controle. Significa que o usuário pode acessar todos, ou quase todos os serviços da rede com um único ID e senha, tal como acesso aos computadores de laboratório, acesso a rede wireless, aplicações etc. Esse recurso facilita para usuários e staff da instituição, porém pode apresentar grande risco

em caso de credenciais vazadas, já que com isso se pode acessar todos os serviços a que o usuário tem acesso com uma única credencial. Métodos mais fortes de identificação e autenticação são recomendados. Também não é recomendado utilizar *secure single sign-on* para funções que exigem alto privilégio.

3.8- Log e monitoramento - Os dispositivos BYOD devem ser constantemente monitorados e o resultado do monitoramento deve ser registrado em forma de logs. Esse monitoramento é importante para ter conhecimento de vários dados do serviço, ter conhecimento de possíveis violações à política de segurança, incidentes e poder tomar ações preventivas. Esses logs podem ser centralizados com o servidor de logs da instituição caso se deseje, facilitando a auditoria dos mesmos.

Alguns destaques para monitoramento relevantes segundo a ISO/IEC 27002 são:

- Todos os relógios de sistemas de informação relevantes na instituição devem ser sincronizados com uma fonte de tempo precisa;
- Identificação dos usuários (ID);
- Datas, horários e detalhes de eventos-chave, como, por exemplo, horário de entrada (*log-on*) e saída (*log-off*) no sistema;
- Identidade do dispositivo ou sua localização quando possível e o identificador do sistema;
- Registros e tentativas de acesso ao sistema, aceitas e rejeitadas;

3.9- Criptografia - A adoção de criptografia é altamente recomendada para garantir confidencialidade, autenticidade e integridade da informação.

Ela deve ser usada para proteger a autenticidade das informações, garantindo que as informações são realmente requisitadas por determinado usuário, o que pode evitar ataques do tipo *man-in-middle* e *spoofing*. Também é importante a adoção de criptografia no método de autenticação dos usuários e dispositivos BYOD aos recursos da instituição como servidor de banco de dados, servidor de arquivos, conexão VPN, etc. Para uma adoção e aplicação de criptografia na instituição, convém a criação de uma Política para uso de controles criptográficos, afim de garantir que o planejamento e utilização da criptografia serão feitos da melhor forma possível.

3.10- Topologia de Rede

Considerando uma instituição de ensino, temos que existe um ambiente administrativo e um ambiente acadêmico, onde são usados os dispositivos BYOD, este onde os usuários alvo atuam (alunos/professores). O ambiente *mobile* deve ser isolado do ambiente administrativo, podendo controlar o acesso dos usuários e evitando que se acesse ou 'enxergue' ativos em redes não desejadas.

Uma boa prática é dividir as redes da instituição em *VLANs*. *VLANs* são redes locais logicamente independentes, elas podem coexistir em um mesmo switch de forma a permitir que uma rede local seja dividida em sub-redes. As principais vantagens de se utilizar *VLANs* estão a topologia de rede independente e aumento de segurança. Essas vantagens citadas são fundamentais para um ambiente *com* dispositivos BYOD, permitindo independência da topologia lógica permitindo que essa rede em específico seja expandida para outros locais sem ficar presa à topologia física, e permite um isolamento lógico dos usuários desse segmento, proporcionando um maior controle por parte do administrador.

É considerado uma boa prática com relação a *VLANs*, criar *VLANs* distintas para perfis diferentes de usuários, facilitando a permissão e negação de acesso. Como exemplo pode-se ter os seguintes perfis:

- **Alunos** - Acessam *Internet* e recursos acadêmicos, como arquivos em um diretório, portal de aulas, vídeos, audios, etc. Esses dispositivos devem estar de acordo com a política de segurança da instituição.
- **Professores** - Acessam *Internet* e os mesmos recursos acadêmicos que o perfil aluno, e ainda possuem permissão de escrita em diretórios de arquivos e portais de conteúdo utilizados para material de aula. Esses dispositivos devem estar de acordo com a política de segurança da instituição.
- **Visitante -** É um perfil criado para uso eventual, por visitantes, palestrantes e afins. Esse usuário deve ter essencialmente acesso à *Internet*.

Outra boa prática com relação à topologia é ter um gateway com filtro de pacotes fazendo o roteamento entre as *VLANs* da instituição**.** A comunicação entre *VLANs*

distintas exige um *gateway* de rede, que na verdade é por onde os pacotes de uma determinada LAN deve passar para se comunicar com outra. Porém para uma maior segurança esse *gateway* deve conter um filtro de pacotes também conhecido como *firewall*, que permite um controle de oque se pode ou não trafegar entre essas sub-redes e *Internet*. É uma boa prática ter um *gateway* com filtro de pacotes pois assim é possível controlar com quais redes os dispositivos móveis podem se comunicar aumentado a segurança e facilitando o controle do administrador. Por exemplo, a instituição de ensino pode permitir que os dispositivos *mobile* na VLAN aluno acesse somente a VLAN de servidores acadêmicos e *Internet*, enquanto o professor acessa ambos e mais alguns recursos da rede administrativa. Para visitantes só é permitido acesso à *Internet*.

Todo esse tráfego é feito pelo *gateway* que faz o roteamento entre todas as sub-redes em questão adicionando um *firewall* para controlar permissões de acesso.

3.11- *Proxy* - Um *proxy* de rede age como um intermediário entre os dispositivos *mobile* e a *Internet*. Ele pode impedir que os dispositivos se conectem diretamente com sites e aplicativos maliciosos de dentro da instituição. Toda requisição do dispositivo passa primeiro pelo proxy, geralmente o gateway da rede, e é ele quem decide a política a ser aplicada, se libera o acesso ou não. São utilizados para bloquear conteúdo web acessados pelo navegador. O uso de *proxy* é interessante devido a segurança que oferece não deixando os dispositivos exporem a rede interna, porém em instituições com um grande número de acessos diários na rede mobile, o uso de um proxy pode exigir uma grande demanda de processamento, podendo causar lentidão a gargalos na rede e tornando seu benefício irrelevante. Uma análise deve ser feita antes de se optar por esse recurso.

3.12- *Backup* - A instituição deve possuir uma política de *backup*. Convém que cópias das informações sejam feitas e testadas regularmente de acordo com a política de backup. Informações como material acadêmico, dados de usuários, registros de log, relatórios da equipe de TI, devem ser regularmente copiados e armazenados em segurança caso seja necessária a recuperação de algum incidente. Essas cópias de segurança (*backup*) devem ser armazenadas em locais seguros e testados regularmente afim de

garantir sua integridade. Algumas considerações em um plano de backup segundo a ISO/IEC 27002 são:

- Proteger os *backups* com criptografia em caso de necessidade de confidencialidade;
- Realizar testes de restauração em uma mídia de teste dedicada, não sobrepondo a mídia original;
- A frequência e abrangência com que os *backups* serão realizados devem atender os requisitos de negócio, de segurança da informação da instituição e criticidade da informação para a continuidade das operações da instituição;

4 CONCLUSÕES

Uma instituição de ensino difere em muitos aspectos de outras instituições no ambiente computacional. Enquanto empresas do setor financeiro ou orgãos governamentais possuem alto sigilo em suas informações, uma instituição de ensino possui um alto número de usuários e tráfego de rede. O ambiente acadêmico de uma instituição pode ser isolado do ambiente que contém dados mais sensíveis (administrativo), o que pode facilitar a vida da equipe de Gestão de Segurança.

Na literatura analisada, ficou claro que nessas instituições o foco em como controlar o acesso dos usuários é mais viável do que a tentativa de monitorar e controlar os dispositivos BYOD utilizados internamente. Por se tratar de um ambiente onde se pode ter centenas e até milhares de usuários conectados diariamente com seus dispositivos pessoais, dispor de recursos com pessoal, treinamentos, hardware/software pode ter um custo caro e não justificável já que em geral os dispositivos não trabalham com dados altamente sensíveis, que necessitem ser mantidos em sigilo. Um *MDM(Mobile Device Managment)*(KEYES,2013) por exemplo permite um monitoramento detalhado de cada dispositivo conectado, porém em geral um ambiente acadêmico não necessita de um grau tão alto de controle fornecido por esse recurso e um investimento nessa ferramenta pode não ser justificado. O mesmo pode-se afirmar para um *firewall* em camada de aplicação, o processamento gerado por tamanho número de requisições de rede não justifica a utilização desse recurso.

O controle de acesso aos recursos e serviços é um caminho viável. Como os usuários que utilizam o ambiente podem ser classificados em perfis, fica simples separar a rede em VLANs específicas para cada perfil e administrar as permissões de acesso necessárias em cada uma e um controle de credenciais bem elaborado e gerenciado permite melhor gerenciamento, monitoramento e auditoria. O acesso depois de autorizado deve ser controlado pela administração, mas não se viu a necessidade de haver um controle rigoroso com ferramentas como o MDM já citado, porém, o plano de tratamento de incidente deve dar conta de possíveis incidentes, como por exemplo ter os backups em dia e um plano de *restore* eficiente.

O mundo de ferramentas para melhorar a segurança de um ambiente mobile está em constante mudança devido à velocidade com que a tecnologia avança nesse campo. Muitas práticas e ferramentas existentes para esses ambientes não se mostraram necessárias para um ambiente acadêmico onde são ministradas aulas e cursos mas, instituições acadêmicas podem também contar com uma ambiente de desenvolvimento de pesquisas, um ambiente cujo acesso de alunos e professores deve ser permitido mas o conteúdo das pesquisas pode ser de absoluto sigilo. Certamente esse ambiente necessita um controle mais rigoroso por parte dos dispositivos BYOD, mas seria conveniente para os usuários ter o ambiente de estudos integrado com esse ambiente de pesquisas, a partir disso novas práticas devem ser levantadas para atender essa necessidade Praticidade X Sigilo.

REFERÊNCIAS

Cisco IBGS – BYOD: Una perspectiva global, 2012.

COMPUTERWORLD, Disponível em <http://computerworld.com.br/negocios/2013/04/09/byod-nao-e-mais-tendencia-no-brasil-diz-gartner/>
Acesso em 07 de abril de 2017.

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 07 abril 2017.

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. Segurança da Informação: o usuário faz a diferença. São Paulo: Saraiva, 2006.

GARANHANI, Bruno. BYOD –Bring Your Own Device ,2013.

SOUPPAYA; SCARFOUNE, Murigiah, Karen. NIST Special Publication 800-124, 2013.

WILL, Daniela. Metodologia da Pesquisa Científica, 2016.

KEYES,Jessica. Bring Your Own Device(BYOD) - Survival Guide, 2013.

TORRES,Gabriel. Redes de computadores 2 Edição, 2014.

ISO/IEC 27001:2013.

ISO/IEC 27002:2013.

ISO/IEC 27033-1:2009.