II Encontro de Iniciação Científica e Tecnológica
II EnICT
ISSN: 2526-6772
IFSP – Câmpus Araraquara
26 e 27 de Outubro de 2017

IMPLEMENTAÇÃO DO BYOD – *BRING YOUR OWN DEVICE* NO AMBIENTE CORPORATIVO PARA O GERENCIAMENTO DE *TABLETS* E *SMARTPHONES*

Fausto Henrique C. Céspedes[1], Juliano Marcelo[2], Fabiana Florian[3]

[1] Graduando em Sistemas de Informação, UNIARA, fausto.cespedes@usinasantafe.com.br
[2] Docente do Curso de Sistemas de Informação da UNIARA, jmarcello@uniara.com.br
[3] Docente do Curso de Sistemas de Informação da UNIARA, fflorian@uniara.com.br

Área de conhecimento (Tabela CNPq): Arquitetura de Sistemas de Computação – 1.03.04.02-9

RESUMO: A popularização de dispositivos móveis e seu uso cada vez mais intenso no ambiente corporativo fez-se surgir mundialmente o fenômeno chamado BYOD (*Bring Your Own Device*) que significa traga o seu próprio dispositivo. O BYOD visa o aumento de produtividade do colaborador da empresa, porém levanta questões relativas a zelar por dados confidenciais da empresa contidos nestes dispositivos e este seria um grande desafio para profissionais da Tecnologia da Informação (TI). Este trabalho tem o objetivo de introduzir o BYOD no ambiente corporativo. Foi realizada pesquisa bibliográfica, documental e de campo em uma empresa do setor sucroenergético na região de Araraquara-SP. Com o uso de uma integração de *softwares* já existentes no mercado (*System Center, Windows Server 2012 e Exchange 2010)* foi possível obter o aumento do nível de controle sobre estes dispositivos pela área de TI da empresa Conseguiu-se realizar algumas ações de segurança tais como o bloqueio de alguns recursos destes dispositivos que não pertencem ao domínio da empresa. Além do bloqueio, foi permitida a opção de apagar todos os dados do dispositivo, em caso de perda ou roubo do equipamento. Esses resultados permitem dizer que a etapa inicial da implementação do BYOD foi eficiente, devido ao aumento da produtividade utilizando dispositivos móveis.

PALAVRAS-CHAVE: BYOD; DISPOSITIVOS MÓVEIS; SEGURANÇA DA INFORMAÇÃO.

INTRODUÇÃO

A popularização da mobilidade resultou em um crescimento irreversível mundialmente, com isso o uso de dispositivos pessoais em todo ambiente, seja ele profissional ou pessoal, trouxe um desafio para as organizações que é conhecido como *Bring your own device* (BYOD) ou seja, “traga seu próprio dispositivo”.

> No mundo todo, 89 por cento dos líderes de TI de grandes empresas e empresas de porte médio apoiam o BYOD de alguma forma. E 69 por cento consideram o BYOD “bastante” ou “extremamente” positivo (IBSG, CISCO, p.03).

O BYOD gera maior produtividade e por se tratar de dispositivos pessoais, cria-se a ideia de um ambiente amistoso para o usuário, levando em conta que muitas vezes o dispositivo pessoal possui um maior número de funcionalidades e um poder de processamento maior que os dispositivos disponibilizados pela corporação.

A implementação de projetos direcionados ao BYOD, pode ser considerada umas das mudanças mais agressivas para os setores de Tecnologia da Informação (TI). “A TI tradicional, acostumada a ter sob domínio o acesso a máquinas passa a fornecer acesso a um grande número de dispositivos, no qual não tem total controle” (MUNIZ, 2013, p.09). Porém o desafio de TI é garantir o menor risco, ameaças e vulnerabilidade na segurança dos dados corporativos.

O objetivo principal deste trabalho foi pesquisar e apresentar os benefícios do início da implantação do BYOD no ambiente corporativo de uma empresa do setor sucroenergético na região de Araraquara-SP.

Esta implantação realiza o gerenciamento dos dispositivos móveis (*tablets, smartphones*), utilizando softwares já existentes *System Center, Windows Server 2012, Exchange 2010,* o que leva a ter um aumento na segurança da informação.

A implantação do BYOD visa garantir o gerenciamento dos dados disponibilizados na rede, o aumento da produtividade do funcionário e um gerenciamento mais abrangente sobre dispositivos móveis no ambiente organizacional.

Foi realizada uma pesquisa bibliográfica com foco em dispositivos móveis - BYOD, seus requisitos de implantação, como políticas bem como a segurança e infraestrutura.

Foi realizada pesquisa documental em que buscou-se realizar um levantamento de informações no banco de dados da empresa. Foi necessário analisar a infraestrutura da empresa visando atender os requisitos mínimos para um adequado funcionamento do sistema.

Também, foi realizado uma pesquisa de campo em uma usina da região de Araraquara-SP.

2 REVISÃO BIBLIOGRÁFICA

2.1 Mobilidade no ambiente de TI

A expansão dos dispositivos móveis aumentou gradativamente entre os usuários com a chegada dos *smartphones e tablets* que incorporam a cada dia novas funcionalidades, tornando-os assim mais parecidos com os computadores tradicionais.

> Além de efetuar chamadas telefônicas, os celulares integraram novas funcionalidades caracterizadas pela convergência midiática, integrando na mesma máquina: computador; câmera digital; acesso à internet; player de música e vídeos; jogos eletrônicos; localização por GPS e outras possibilidades de interação, produção e acesso de conteúdo. Além disso, é um dispositivo portátil e com mobilidade, possibilitando a criação e acesso de conteúdos em movimento (PEREIRA, 2014, p.02).

A tradicional área de tecnologia da informação da empresa busca atender os objetivos atribuídos pela organização, utiliza-se seus próprios recursos de maneira eficaz. A área de TI das organização acostumadas a ter total domínio sobre estes recursos, ganha uma mudança de cenário e necessita atender e gerenciar conexões de dispositivos que estão fora de seu ambiente de domínio:

> Enquanto a área de TI corporativa tem se preocupado em alinhar os recursos de informática com os objetivos organizacionais, os funcionários utilizam cada vez mais equipamentos e aplicativos não controlados pela TI, na busca de soluções mais próximas de suas necessidades (FELICIANO; MAÇADA, 2013, p.03).

2.2 Políticas de Segurança da Informação

A política de segurança da informação descreve a filosofia e as regras básicas para o uso do recurso da informação (DANTAS, 2011). Com a existência da política fica explicitado o que cada pessoa da organização deve cumprir no que se refere à proteção da informação (FONTES, 2008).

A segurança da informação vem se tornando um assunto de importância entre empresas, devido ao avanço tecnológico e grande competitividade de mercado, o que cria a necessidade da aplicação de políticas claras e um sistema de informação seguro.

> Para LAUDON (2007), citado por (IETSUGU; SIMÂO, 2013, p.09) as empresas estão sempre tentando melhorar a eficiência de suas operações a fim de conseguir maior lucratividade. Das ferramentas de que os administradores dispõem, as tecnologias e os sistemas de informação estão entre as mais importantes para atingir altos níveis de eficiência e produtividade nas operações.

2.3 BYOD

O BYOD é um fenômeno mundial que vem crescendo a cada dia, usuários deixam seus computadores de mesa, e iniciam uma nova etapa, a etapa da diversidade de dispositivos, o que dificulta o suporte para equipes de TI.

> O aumento de conexões resultantes da tecnologia móvel no país tem proporcionado diferentes oportunidades e desafios aos hábitos sociais e aos limites entre espaços públicos e privados (LEMOS, A; JOSGRILBERG, F, 2009, p.11).

Para (IBSG, Cisco), gostando ou não, as empresas entraram em um "mundo pós-PC", no qual a rede deve acomodar novas opções. Essas opções incluem aplicativos sociais e sistemas operacionais tradicionais, móveis e sociais, diversas arquiteturas de servidor e uma ampla gama de dispositivos móveis, desde smartphones a tablets e outras ferramentas de mobilidade.

Segundo a empresa Cisco (IBSG), foram entrevistados 4.892 funcionários de nove países (Estados Unidos, Reino Unido, Alemanha, França, Rússia, China, Índia, México e Brasil), quanto aos quesitos: produtividade/colaboração, satisfação no trabalho e custos reduzidos. Observou-se um aumento expressivo na produtividade e ocorreu a colaboração do funcionário a partir do momento em que se inicia o uso de seus próprios dispositivos.

De acordo com a IBSG, o colaborador acaba se sentindo mais satisfeito, pois, deixa de ser obrigado a utilizar um dispositivo fornecido pela empresa (que nem sempre atende suas expectativas), e passa a poder trabalhar com seu próprio dispositivo, que muitas vezes possui um melhor desempenho. Um dado negativo é a falta de políticas de segurança e de acesso bem definidas nas empresas para tratarem o BYOD.

3 ESTUDO DE CASO EM UMA USINA NA REGIÃO DE ARARAQUARA-SP

Foi realizado estudo na área de TI (infraestrutura) em uma usina do setor sucroenergético da região de Araraquara-SP.

3.1 Identificação do local de implementação

O processo de implantação do BYOD ocorreu no ambiente empresarial na área administrativa e área agrícola utilizando rede cabeada e wireless em diversos pontos da empresa, ou conexão 3G ou 4G.

Foi utilizada uma solução da *Microsoft* (*System Center*), para realizar o gerenciamento inicial de dispositivos móveis na empresa. Buscou –se alcançar parâmetros de segurança dentro da empresa, como bloqueios de determinadas funções do aparelho como câmera e criptografia dos dados do celular. Este processo levou cerca de dois meses.

3.2 Identificação do Usuário

A identificação utiliza usuários criados no *Active Directory*, para acesso à impressão e acesso à internet, já para um gerenciamento mais profundo de dispositivos móveis, foi utilizada uma conta de e-mail no servidor do *Exchange* da empresa.

3.3 Topologia

Com o uso da ferramenta *System Center* da *Microsoft*, foi realizada a implementação inicial de controle do dispositivo, assim o administrador do domínio pode efetuar determinadas ações como bloquear o uso da câmera, ou roteamento de rede via celular, ou até mesmo apagar todos os dados do dispositivo em um caso de perda ou furto do equipamento com informações corporativas.

3.4 Ferramentas

A usina já possui todo o ambiente de infraestrutura de rede montado, com licença do *software System Center, Windows Server 2012, Exchange 2010* e o domínio usinasantafe.com.br registrado.

3.5 Permissões de acesso

Todo o acesso é gerenciado pelos usuários administradores do domínio, apesar de dispositivos geralmente serem configurados por integrantes da infra-estrutura da TI da empresa, basta apenas que, a conta de e-mail seja adicionada ao dispositivo para fazer parte de uma regra de acesso no *System Center*, e assim passar a ter funcionalidades gerenciadas como câmera, criptografia, *wireless*, *bluetooth* dentre outros.

Ao configurar o conector do *System Center* com o *Microsoft Exchange*, foi definido o tipo de acesso e bloqueios a determinadas funcionalidades de aparelhos (Figura 1).

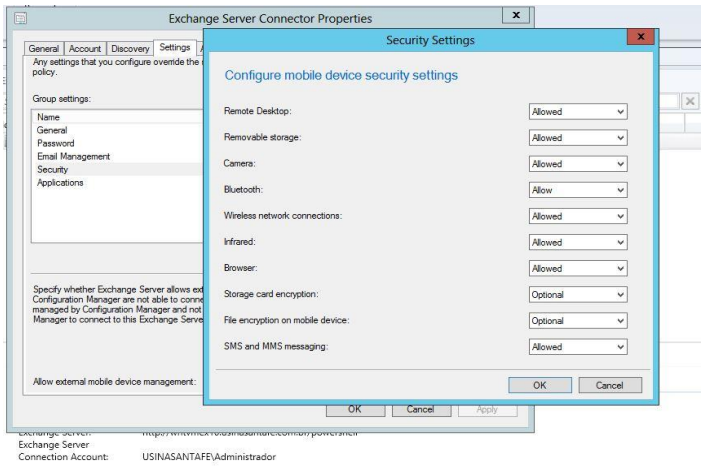

FIGURA 1. Configuração do *Exchange Connector*
Fonte: o autor.

Na figura 1 foi definido uma configuração padrão para todos os dispositivos que se conectam por meio de uma conta de e-mail ao dispositivo. Na aba *Access Roles*, há diferentes categorias, com diversos

parâmetros de acesso, conseguindo assim criar perfis para diversos tipos de funcionários como desde um diretor ou gerente, até um auxiliar administrativo que possui funções mais restritas na empresa (definimos o que ele poderá utilizar em seu dispositivo móvel).

Foi criado um perfil padrão (*All mobiles devices*), este perfil possui acesso mais restrito a funcionalidades no seu dispositivo, assim qualquer dispositivo que seja configurado entra automaticamente neste perfil de acesso.Com o dispositivo configurado, o administrador do domínio pode gerencia-lo, movendo para outras regras de acesso, como regras para gerentes e outros (Figura 2).

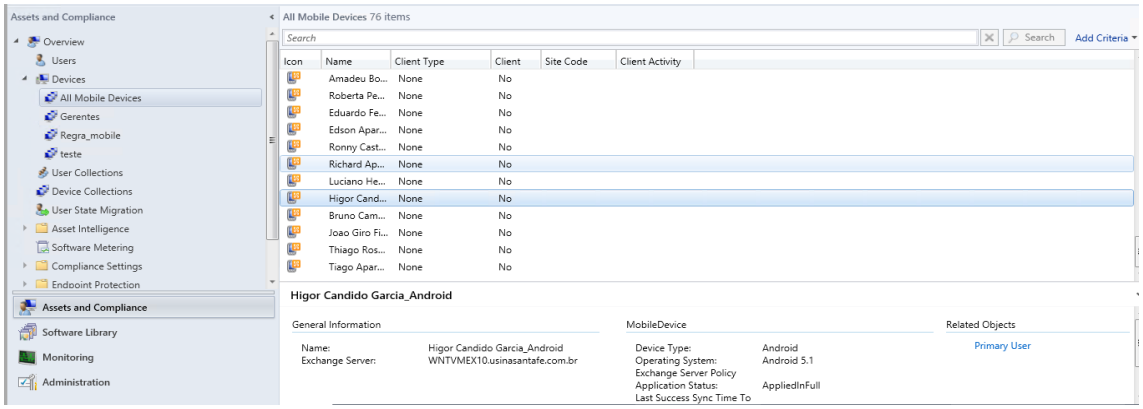

FIGURA 2. Grupos de acesso
Fonte: o autor.

3.6 Riscos Iniciais

No cenário apresentado na empresa, ocorre um grande risco no caso de perdas do equipamento e de informações, já que no momento possuímos um alto número de usuários incluindo nível de gerencia da empresa.

3.7 Resultados

Obteve-se um ganho expressivo, o número de smartphones e tablets nestes últimos dois anos, passou de 30 dispositivos no início, para mais de 400 atualmente. Hoje estes dispositivos acessam informações como consultas de moagem por hora, estoque de cana no pátio, qual a produção diária, valores no mercado. (Consultas gerenciais).

Também enviam informações de apontamento, por meio de um aplicativo desenvolvido internamente instalado no smartphone, envia motivos de parada de um equipamento, qual local está operando dentre outros dados.

Este tipo de gerenciamento não possui acesso a arquivos e informações pessoais contidas nos dispositivos, diferente de outras soluções como o Microsoft Intune, que possui um acesso mais amplo, porem depende de instalação de aplicativo no dispositivo para operar.

Conforme adicionava-se as contas de usuário do A*ctiveDdirectory* aos tabletes e smartphones, foi realizado um treinamento, para explicar como ocorria o funcionamento, e assim foi elaborado um questionário a fim de obter o nível de aceitação dos gerentes e outros profissionais sobre o uso de dispositivos móveis no ambiente corporativo. O Quadro 1 apresenta as questões que foram aplicadas as áreas administrativa e agrícola envolvendo um total de 10 participantes.

Questões	SIM	NÃO
1. O uso de dispositivos pessoais atrapalha no desempenho das funções internas do funcionário na empresa?	3	7
2. O avanço tecnológico ajuda nas tarefas do funcionário?	9	1
3. O uso de dispositivos móveis pessoais dentro da empresa ainda é uma barreira a ser quebrada?	8	2
4. A empresa realizar o gerenciamento sobre estes dispositivos pessoais gera uma maior tranquilidade a nível de gerencia da empresa?	10	0
5. Com a implantação do BYOD, acredita que os dados, tanto pessoais como coorporativos estão mais seguros?	8	2

QUADRO 1.Questionário aplicado na empresa sobre a aprovação do uso de dispositivos móveis no ambiente corporativo.
Fonte: o autor.

4 CONSIDERAÇÕES FINAIS

O avanço ocorrido nos últimos anos no ramo da tecnologia da informação, vem trazendo uma grande expectativa tanto para gerentes de TI, quanto para funcionários da empresa, que passam a utilizar dispositivos moveis no seu dia a dia corporativo esteja ele em seu local de trabalho, ou em sua casa, podendo acompanhar e utilizar informações da empresa.

Com a utilização desta implantação, obteve-se o aumento na segurança das informações da empresa, maior flexibilidade ao gerenciar vários tipos de dispositivos, opções como apagar dados contidos no dispositivo e boquear recursos do dispositivo.

BYOD se torna uma realidade a cada dia, basta apenas as empresas conseguirem encontrar uma melhor maneira de absorver seus benefícios, e principalmente tratar seus riscos, sejam eles jurídicos ou de segurança da informação.

5 REFERÊNCIAS

DANTAS, M. L.. **Segurança da informação: uma abordagem focada em gestão de riscos.** Olinda – PE, 2011. Acessado em: Disponível em: http://www.marcusdantas.com.br/files/seguranca_informacao.pdf 25/05/2016.

Feliciano, Sidnei, Maçada, Antonio C. G., "**Impactos da Consumerização de TI no Desempenho e na Governança de TI**" (2013). CONF-IRM 2013 Proceedings.Paper 37.

FONTES, E. L. G. **Praticando a segurança da informação.** Rio de Janeiro: Brasport, 2008.

IETSUGU, M.; SIMÂO, D. **A Segurança da informação nas empresas de ourinhos e região:** um estudo de caso. Ourinhos, 2013.

Internet Business Solutions Group (IBSG), Cisco. **BYOD: uma perspectiva global**. Disponível em: https://www.cisco.com/c/dam/en_us/about/ac79/docs/re/byod/BYOD_Horizons_Global_PTBR.pdf Acesso em: 20/05/2016.

LAUDON, Kenneth & LAUDON, Jane. **Sistemas de informação gerenciais**. 7.ed São Paulo: Pearson Pratice Hall, 2007.

LEMOS, A; JOSGRILBERG, F. **Comunicação e mobilidade:** aspectos socioculturais das tecnologias móveis de comunicação no Brasil. UDUFBA, Salvador, 2009.

PEREIRA, Liliane Aparecida. **Smart Mob.** 9^0 Interprogramas de Mestrado em Comunicação da Faculdade Cásper Líbero, São Paulo – SP, 2014.