Gestão da Segurança da Informação em ambientes BYOD: Um mecanismo de apoio baseado nas boas práticas ITIL

I. K. B. Cunha, R. C. C. Castro

Grupo de Pesquisa em Informática Aplicada - Instituto Federal de Educação, Ciência e Tecnologia (IFCE) – Canindé, CE - Brasil.

kariseilane@gmail.com, ritacastro@ifce.edu.br

Abstract*. The complexity of environments processes supported by the Information Technology and Communication is increasing by leaps and bounds with the insertion of practices such as BYOD, which, on the other hand, is driven by the proliferation of personal mobile devices in the corporate environment. This scenario, when not controlled by strategies arising from the IT Governance can cause the ruin of business. This paper aims to present a mechanism to support companies or organizations wanting to join BYOD, enables them to align the tendency to managing information security, through the application of best practices in IT Governance Framework ITIL V3 constant.*

Resumo*. A complexidade dos ambientes suportados pelos processos da Tecnologia da Informação e Comunicação vem aumentando a passos largos com a inserção de práticas como o BYOD, que, por sua vez, é impulsionada pela proliferação dos dispositivos móveis pessoais no ambiente corporativo. Este cenário, quando não controlado por estratégias oriundas da Governança de TI pode representar a ruína do negócio. O presente trabalho tem por objetivo apresentar um mecanismo de apoio às empresas ou organizações que pretendem aderir ao BYOD, possibilitando aos mesmos o alinhamento da tendência à gestão da segurança da informação, através da aplicação de boas práticas de Governança de TI constante no framework ITIL V3.*

1. Introdução

Durante anos diversas empresas mantinham seus negócios com pouco ou nenhum apoio da equipe de Tecnologia da Informação e Comunicação (TIC). Atualmente essa realidade mudou, e não poderia ser diferente, pois a TI tornou-se um fator crítico de sucesso para as organizações, e, em muitos casos, o principal diferencial competitivo no mercado.

Considerando essa competitividade e a criticidade da informação para alguns órgãos, a gestão dos ativos da informação acaba despontando como um processo dos mais importantes. Desta forma, a gestão corporativa de TI, deve, através de um modelo bem definido e estruturado, ser integrada e alinhada ao planejamento estratégico da empresa, possibilitando a esta a capacidade de adaptar-se rapidamente às necessidades de mudanças do negócio, evitando que novos serviços e alterações em serviços já existentes sejam implantados de forma errônea ou de maneira que infrinjam os controles da empresa, mitigando assim os riscos aos ativos de informação. Toda essa estrutura de relações e processos encontra-se inserida na Governança de TI.

Surge atualmente no cenário corporativo uma nova tendência denominada BYOD – *Bring your own device* [CIO, 2013], em português “Traga seu próprio

dispositivo", caracterizada pela entrada dos mais variados tipos de dispositivos móveis pessoais nas empresas trazidos pelos próprios funcionários, para ser aproveitado no meio corporativo como ferramenta de trabalho, deixando o colaborador livre para escolher e comprar o dispositivo que queira utilizar em suas tarefas no âmbito organizacional.

As empresas ou organizações que desejam usufruir das vantagens do BYOD devem estar preparadas para administrar todos os desafios relacionados à sua implantação, possibilitando assim colocar sistemas e práticas no ambiente corporativo de forma eficiente, garantindo serviços previsíveis, confiáveis, que não comprometam a integridade dos ativos da informação. Visando isso, é fundamental que estejam inseridas nas organizações aderentes à tendência, boas práticas de Governança de TI, principalmente relacionadas à segurança da informação.

Embora pesquisadores e estudiosos da área, reconheçam a importância da Governança de TI e seu papel nas organizações, a forma de implementá-la ainda é um desafio, pois dependendo dos objetivos estratégicos da empresa, se faz necessário adotar abordagens diferenciadas em cada caso. A sua aplicação em empresas ou órgãos que aderiram à tendência BYOD torna-a ainda mais específica, uma vez que não há casos documentados na literatura.

Este artigo vem propor a aplicação de boas práticas de Governança de TI em ambientes coorporativos e organizacionais, que venham a aderir ao BYOD, possibilitando que sua aplicação esteja alinhada a gestão coorporativa e a segurança da informação da organização, através da aplicação de conceitos de Gerenciamento da Segurança da Informação constante no *framework Information Technology Infrastructure Library Version three* (ITIL V3).

2. Governança de TI – Marco Teórico

A Governança de TI adquiriu ao longo dos anos diversas definições diferenciadas na literatura. Analisando um retrospecto, da mais remota a mais atual, pode-se perceber que quase todas abordam a forma de autoridade da tomada de decisão de TI na organização (estrutura) e a forma com que os recursos de TI são gerenciados e controlados (processos), buscando sempre alinhar os investimentos realizados em TI às estratégias corporativas.

Venkatraman, em 1991, [apud LOH, 1993] definiu-a como sendo um sistema baseado em TI utilizado para descrever como esta media ou governava os relacionamentos de negócios.

Em 1992, Henderson e Venkatraman [apud LOH, 1993] ampliaram a definição anterior de forma que abrangesse escolhas de mecanismos estruturais, tais como *joint ventures*, contratos de longo prazo e boas parcerias, que seriam utilizadas para obter capacidades requisitadas da TI.

Sete anos mais tarde Sambamurthy e Zmud [1999] definiram-na como sendo a implementação de estruturas e arquiteturas relacionadas à TI para atingir com sucesso atividades em resposta ao ambiente e a estratégia organizacional.

Na definição proposta por Korac-Kakabadse e Kakabadse [2001] a Governança de TI passa a se concentrar também na necessidade de definir processos e mecanismos de relacionamento (e não apenas estruturas) para desenvolver, dirigir e controlar os recursos de TI, de modo a atingir os objetivos da organização.

Segundo Fernandes e Abreu [2008], os escândalos e fraudes corporativos, bem como as crise financeira mundial, foram observadas pelos atentos olhos dos acionistas e investidores, que passaram a exigir mais exatidão nas previsões orçamentárias das empresas aos quais eram ligados, como também maior transparência no que se refere aos gastos e retornos financeiros. Essa mudança comportamental alavancou a Governança de TI e tornou-a um tema dominante nos negócios, devido ao impacto dos gastos realizados na implantação de novas tecnologias no ambiente coorporativo.

3. ITIL

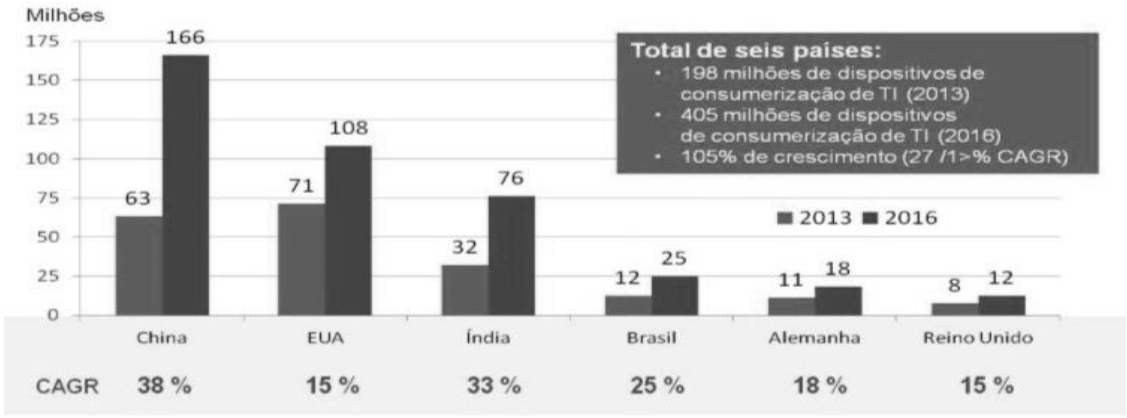
Toda organização enfrenta problemas relacionados à tecnologia, que causam impactos negativos aos diversos entes envolvidos no negócio e principalmente à própria organização, prejudicando as atividades desenvolvidas por ela. Possuir um plano para administrar esses eventos negativos e lidar com as situações de crise de maneira padronizada, alinhada e estruturada é um fator primordial. A equipe estratégica deve saber como proceder antes, durante e depois de um incidente.

Magalhães e Pinheiro [2007] definem o ITIL V3 como um guia de procedimentos e boas práticas que promove às empresas uma estrutura (*framework*) abrangente e detalhada para o gerenciamento de serviços de TI. Ele aborda os serviços de TI durante todo o seu ciclo de vida e sugere cinco fases, contendo todos os mecanismos, para que o gerenciamento seja realizado de maneira adequada em todas as suas fases, possuindo uma visão voltada para a alta qualidade de serviços na origem e na entrega, bem como que estes estejam em conformidade com a legislação e ainda que se gere um ciclo contínuo para melhorá-los.

As boas práticas sugeridas pelo ITIL podem ser utilizadas por qualquer organização pelo fato de não se basear em nenhuma plataforma proprietária, bem como aplicadas a qualquer tipo de empresa, do setor privado ou público, de pequeno, médio ou grande porte, e são frutos das experiências e ideias das maiores lideranças na área de gerenciamento de serviços de TI.

4. BYOD

Pesquisas atuais apontam que a tendência em se adotar a prática do BYOD tem ganhado regiões como China, Índia e Oriente Médio, confirmando a abrangência do fenômeno. Segundo o relatório da CISCO IBSG [2013], pelo menos 89% dos departamentos de TI já permitem a sua utilização. Esse mesmo relatório afirma que a tendência é um fenômeno crescente e de grandes proporções. Nos países analisados (figura 1), o número de dispositivos utilizados no âmbito corporativo aumentará 105% entre 2013 e 2016, atingindo aproximadamente 405 milhões, o que resulta uma taxa de crescimento composto anual (CAGR) de 27%.



Fontes: EIU, Strategy Analytics, Cisco IBSG, 2013

Figura 1. Número estimado de dispositivos de consumerização de TI nos locais de trabalho, por país.

No Brasil o fenômeno surgiu em meados de 2011, advindo da cultura coorporativa internacional [PLÁCIDO, 2011], e notoriamente impulsionada por um conjunto de fatores: surgimento da computação móvel, expansão dos dispositivos móveis, facilidade na aquisição de novas tecnologias e o ingresso da população nova, conhecida como geração digital e aficionada por novas tecnologias, no mercado.

A cada momento existe uma adequação das novas tecnologias que surgem com a estratégia das empresas em que são inseridas. No BYOD há diversos fatores que impulsionam a sua adoção dentro das organizações: maior produtividade, flexibilidade, satisfação do funcionário, redução dos custos para a empresa, dentre outros.

Entretanto, apesar das inúmeras vantagens trazidas pelo efeito BYOD, há também uma série de desafios a serem enfrentados diariamente, onde a maioria destes está relacionada à segurança da informação.

5. Alinhamento do BYOD ao Gerenciamento da Segurança da Informação

Sendo a TI um dos principais componentes de qualquer organização, a Governança de TI torna-se um assunto de grande relevância para a alta administração. Os riscos referentes às tecnologias adotadas, assim como o seu desempenho, a sua relação com as estratégias corporativas e, ainda, as políticas e responsabilidades ligadas a TI certamente irão afetar a organização, em uma maior ou menor proporção. Uma simples quebra de segurança, um erro ou um ataque de vírus já é suficiente para causar um sério prejuízo financeiro, e de reputação e imagem à organização [HARDY, 2006].

A implementação de boas práticas dentro da estratégia organizacional permite uma gestão mais profissional e transparente de modo a maximizar a criação e agregação de valores dentro das empresas. Geralmente quando se fala em implementação de governança, esta pode ser iniciada, em alguns casos, em virtude de um interesse específico (como, por exemplo, definir estratégias e procedimentos que viabilizem a adesão do BYOD dentro das empresas) ou pela presença de problemas críticos para a organização (como os problemas decorrentes da implementação do BYOD, tais como: lidar com diversos sistemas operacionais, segurança de dados coorporativos, controle de acesso de usuário, dentro outros).

Diferentes pesquisadores têm respondido a essa questão sugerindo que é necessário combinar um conjunto de práticas referentes à estrutura, processos e

mecanismos de relacionamento para se obter excelência no que diz respeito a uma implementação eficaz e de qualidade [PETERSON, 2004; VAN GREMBERGEN, DE HAES e GULDENTOPS, 2004; WEILL e WOODHAM, 2002]. Lunardi et. al. [2007], afirma que esses mecanismos, por sua vez, não precisam necessariamente ser utilizados na sua totalidade ou da mesma forma pelas organizações, pois uma série de características da própria empresa ou negócio de atuação pode exigir diferentes configurações, evidenciando a complexidade na determinação dos mecanismos mais indicados a serem adotados.

O Gerenciamento da Segurança da Informação tem total alinhamento à norma ISO/IEC 17799 ou ABNT NBR ISO/IEC 27001. Esse processo visa gerenciar efetivamente a segurança da informação em todas as atividades do serviço, abordando a avaliação de riscos para os ativos conforme sua criticidade, o estabelecimento de controles para garantir a segurança e a disponibilidade da informação e o tratamento de mudanças e incidentes de segurança, em conformidade com os requisitos de segurança exigidos pelo negócio. A norma aponta claramente quais são os controles considerados como melhores práticas para a segurança da informação:

- Documento da política da segurança da informação: tem como objetivo prover à direção uma orientação e apoio para a segurança da informação;
- Definição das responsabilidades na segurança da informação: objetivando gerenciar a segurança da informação na organização;
- Educação e treinamento em segurança da informação: com o intuito de assegurar que usuários estejam cientes das ameaças e das preocupações de segurança da informação e estejam equipados para apoiar a política de segurança da organização durante a execução normal do seu trabalho;
- Relatório dos incidentes de segurança: tem como objetivo minimizar os danos originados pelos incidentes de segurança e mau funcionamento, e monitorar e aprender com tais incidentes;
- Gestão da continuidade do negócio: com o objetivo de não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos.

É importante ressaltar que mesmo com todas as melhores práticas já catalogadas nas normas e nas bibliotecas de gerenciamento, recomenda-se que as organizações adaptem as práticas ITIL conforme seu contexto, e defendam suas próprias melhores práticas no âmbito da estrutura global de gerenciamento de serviço.

6. Proposta de *check-list*

Visando à adoção do BYOD e com o intuito de remediar possíveis vulnerabilidades no âmbito da segurança da informação, este trabalho propõe a adoção de um *check-list* (Tabela 1) baseado nas boas práticas do Gerenciamento da Segurança da Informação – conforme apresentadas no tópico anterior – acrescentando-se, necessariamente, um tópico, a fim de nortear a equipe de TI antes da adoção dessa nova tendência dentro do ambiente corporativo.

Tabela 2 - Proposta de Check-List

ITEM	QUESTÃO	S/N
1.	**Documento da Política de Segurança da Informação**	
1.1.	A empresa/organização possui um documento de "Política de Segurança da Informação"?	
1.2.	O documento contém a definição de segurança da informação, resumo das metas e escopo e a importância da segurança como um mecanismo que habilita o compartilhamento da informação?	
1.3.	O documento comtempla todas as políticas, princípios, padrões e requisitos necessários para o bom funcionamento da empresa/organização?	
1.4.	O documento está em conformidade com a legislação e todas as clausulas contratuais que a empresa tem com os seus fornecedores e parceiros?	
1.5.	O documento é fortemente implementado na empresa?	
1.6.	Quando um princípio é violado as consequências constantes no documento são devidamente aplicadas?	
1.7.	A política da informação é acessível, compreensível e conhecida por todos os funcionários?	
1.8.	Há alguma modificação que necessita ser revista na política de segurança da informação já existente?	
1.9.	As modificações necessárias são aplicadas?	
2.	**Definição de responsabilidades na segurança da informação**	
2.1.	Há uma definição das responsabilidades gerais e específicas na gestão da segurança da informação?	
2.2.	As responsabilidades pela proteção de cada ativo são claramente definidas?	
2.3.	As responsabilidades pelo cumprimento de processos de segurança são claramente definidos?	
2.4.	A empresa adota um processo de gestão de autorização para utilização de novos recursos computacionais?	
2.5	A empresa possui uma política de adesão e utilização de novas tecnologias?	
3.	**Educação e treinamento em segurança da informação**	
3.1.	A empresa oferece uma educação suficiente aos seus funcionários relacionada à segurança da informação?	
3.2.	As recomendações sobre segurança da informação estão sendo transmitidas de forma eficaz?	
3.3.	A empresa adota mecanismos suficientes para que os funcionários fiquem cientes sobre os riscos a que estão expostos quando da utilização de novas tecnologias?	
3.4.	A empresa realiza treinamentos para instruir os seus profissionais ao uso de boas práticas na utilização dos dispositivos móveis?	
4.	**Relatórios dos incidentes de segurança**	
4.1.	A empresa oferece uma Central de Serviços para que os usuários possam reportar incidentes de segurança da informação?	

4.2.	A Central de Serviços oferece um feedback notificando aos usuários sobre os resultados obtidos após o incidente ser tratado e encerrado?	
5.	**Gestão de continuidade do negócio**	
5.1.	A empresa/instituição identificou os eventos que podem causar interrupções nos processos de negócio no caso da autorização de utilização de dispositivos móveis dentro do ambiente corporativo?	
5.2.	A empresa/instituição entende os riscos a que está exposta quando da adesão do BYOD?	
5.3.	Há algum tipo de documentação de estratégia de continuidade consistente com objetivo e prioridades estabelecidas para o negócio em caso de interrupções dos serviços?	
6.	**Mecanismos de segurança BYOD**	
6.1.	A empresa possui tecnologia que faz com que o nó realize autenticação ao se conectar à rede?	
6.2.	A empresa dispõe de um controle de acesso de usuário que abranja os dispositivos móveis?	
6.3.	A empresa está preparada para proteger os dados corporativos em todos os dispositivos pessoais utilizados na prática BYOD?	
6.4.	A empresa adota mecanismos de controle sobre os dispositivos, para utilização em casos de desligamento do funcionário da empresa?	

7. Conclusão

O avanço das Tecnologias da Informação e Comunicação e a importância da informação na sociedade fazem com que práticas como o BYOD comecem a ser difundidas no meio corporativo, garantindo a flexibilidade na utilização de dispositivos móveis e pessoais no ambiente de trabalho.

Todos os aspectos abordados nesta pesquisa não esgotam o tema dos desafios associados ao BYOD, já que a sua adoção e prática, aqui no Brasil, ainda está se desenvolvendo. Por conta disso, a alta administração é constantemente indagada ao adotar uma tendência que ainda é nova no mercado, pois a informação é tratada atualmente como um dos ativos mais importantes dentro da estrutura organizacional.

Através do *check-list* proposto, o administrador, juntamente com sua equipe estratégica e o departamento de TI, poderá adequar a empresa ou instituição a todos os pontos que já são considerados como boas práticas para a segurança da informação. E somente depois que todos os itens estiverem inseridos dentro da organização adotar a nova tendência.

É importante ressaltar que o *check-list* proposto não se trata de um modelo fechado e adequado para qualquer tipo de instituição, visto que a própria Governança de TI recomenda que as organizações adaptem as práticas, conforme seu contexto, e, também, que elas defendam suas próprias melhores práticas. Isso faz com o *check-list* seja tratado de modo genérico e norteador para as instituições que o desejem utilizar.

Como proposta para trabalhos futuros, sugere-se uma avaliação sistemática dos riscos de segurança da informação quando da adoção do BYOD. Através desta avaliação poderão ser identificadas as ameaças e as vulnerabilidades a que estão

expostos os ativos, como também a probabilidade de ocorrência e a estimativa das potenciais consequências do impacto nos negócios da organização.

8. Referências

CIO - **BYOD to Change the Face of IT in 2013.** Consumer Tech, Publicado em: 7 fev. 2013. Disponível em: http://www.cio.com/article/728487/BYOD_to_Change_the_Face_of_IT_in_2013 Acesso em: 19 de ago. 2014.

CISCO Internet Business Solutions Group IBSG. **O impacto financeiro da consumerização de TI.** Disponível em: <http://www.cisco.com/web/about/ac79/docs/re/byod/BYOD - Economics_Economic-Analysis_BR.pdf > Acesso em: 19 de ago. 2014.

FERNANDES, Aguinaldo Aragon; ABREU, Vladimir Ferraz de. **Implantando a governança de TI: da estratégia à gestão dos processos e serviços.** 3ª ed. Rio de Janeiro: Brasport, 2012.

HARDY, G. **Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges.** Information Security technical report, 2006, pp. 55-61.

KORAC-KAKABADSE, N.; KAKABADSE, A. **IS/IT governance: need for an integrated model.** Corporate Governance, v. 1, n.4, 2001.

LOH, L. **The economics and organizational of information technology governance: sourcing strategies for corporate information infrastructure.** Massachusetts, 1993. Tese (Doutorado em Administração) – Alfred P. Sloan School, Massachusetts Institute of Technology, MIT.

LUNARDI, G. L.; DOLCI, P. C.; BECKER, J. L.; MAÇADA, A. C. G.; **Governança de TI no Brasil: uma análise dos mecanismos mais difundidos entre as empresas nacionais.** SEGeT – Simpósio de Excelência em Gestão e Tecnologia. 2007.

MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito - **Gerenciamento de serviços de TI na prática: uma abordagem com base no ITIL.** Série Gerenciamento de TI. São Paulo: Editora Novatec, 2007.

PETERSON, R., **Integration strategies and tactics for information technology governance.** In: VAN GREMBERGEN, W. Strategies for information technology governance, Hershey: Idea group publishing, 2004.

PLÁCIDO, Daniel Gonçalves; Araújo Júnior, Edson. **Consumerização e a Continuidade do Negócio**. Info Educativa. Publicado em dez, 2011. Disponível em <http://www.infoeducativa.com.br/index.asp?page=artigo&id=929> Acesso em: 15 de ago. 2013.

SAMBAMURTHY, V.; ZMUD, R. **Arrangements for information technology governance: a theory of multiple contingencies.** MIS Quarterly , v. 23, n. 2, 1997.

VAN GREMBERGEN, W.; DE HAES, S.; GULDENTOPS, E. **Structures, processes and relational mechanisms for IT governance.** Strategies for information technology governance, Hershey: Idea group publishing, 2004.

WEILL, P.; WOODHAM, R. **Don't just lead, govern: implementing effective IT governance.** Center for Information Systems Research . Working paper n. 326, 2002.