A APLICAÇÃO DA GOVERNANÇA E GESTÃO DA SEGURANÇA DA INFORMAÇÃO NA DEFINIÇÃO DE DIRETRIZES PARA UTILIZAÇÃO DA SUÍTE COLABORATIVA DO OFFICE 365: ESTUDO DE CASO [1]

Ricardo da Silveira[2]

Resumo: A segurança da informação está despertando a atenção das empresas de um modo geral, haja vista que ela está diretamente ligada à imagem da organização, à vantagem competitiva e à continuidade de seus negócios. Pela importância desses fatores, com o intuito de preservar a robustez dos negócios, este trabalho apresenta um diagnóstico sobre a segurança das informações armazenadas na ferramenta colaborativa Office 365. Baseando-se em referências bibliográficas e na realização de uma pesquisa, foi possível identificar pontos importantes de vulnerabilidade, bem como foram sugeridas melhorias para o ambiente. Conclui-se que é de suma importância que projetos sejam conduzidos com seriedade e que envolvam as pessoas e as áreas afetadas tanto direta como indiretamente, para que o negócio se torne seguro e produtivo, mitigando os riscos.

Palavras-chave: Segurança. Informação. Riscos. Governança. Segurança da Informação.

1 INTRODUÇÃO

O surgimento de novas ferramentas colaborativas ancoradas em nuvem vem revolucionando a Tecnologia da Informação em muitos sentidos, tendo em vista que são muitas as facilidades que elas vêm proporcionando para as organizações e também para a rotina dos seus colaboradores.

É válido ressaltar que a aderência às novas ferramentas rompe com o tradicionalismo de determinadas funções da empresa, fazendo com que estas estejam mais à frente do mercado comum, garantindo a ampla competitividade.

---

[1] Artigo apresentado como Trabalho de Conclusão do Curso de Especialização em Gestão da Segurança da Informação, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Gestão da Segurança da Informação.

[2] Acadêmico do Curso de Especialização em Gestão da Segurança da Informação. E-mail rsilveira88@yahoo.com.br.

Toda essa transformação digital está gerando um rompimento no modo tradicional de como as informações são centralizadas e no modo como a segurança é tratada; com essa transformação, os acessos a esses conteúdos acabam ficando mais vulneráveis e naturalmente menos concentradas. Para que os usuários possam fazer o uso dessas novas ferramentas considerando os princípios de colaboração e dinamismo proposto por elas, é indispensável e ao mesmo tempo natural que o utilizador receba mais permissões e autonomia para disseminar os acessos e gerar compartilhamentos.

Este trabalho é essencial para demonstrar que a organização pode usufruir dos benefícios das ferramentas colaborativas do Office 365 proporcionando uma maior agilidade e qualificando ainda mais o trabalho de seus colaboradores sem comprometer a segurança dos seus dados e informações.

De acordo com Campos (2007), a informação é um componente essencial para os processos de negócio da organização, sendo um bem ou ativo de grande valor. Logo, a informação se tornou o ativo mais valioso das organizações, podendo ser ameaçado de diversas formas. Por essa razão, se faz necessária a implementação de políticas e boas práticas de segurança da informação que busquem reduzir as chances de fraude ou perda das informações.

Na visão de Sêmola (2003), “realizar uma análise de segurança já é prioridade para a grande maioria das empresas, o que vem demonstrar a percepção da necessidade de diagnosticar os riscos”. Sêmola (2003) ainda define a segurança da informação “como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

Neste sentido, podemos elencar como um dos objetivos básicos da segurança da informação a diminuição dos impactos provocados na organização para um nível aceitável de risco, bem como proteger os ativos de informações contra o risco de perda, descontinuidade operacional, uso indevido, divulgação não autorizada, indisponibilidade e danos (ITGI, 2006).

O trabalho visa a busca de dados relativos à segurança da ferramenta colaborativa do Office 365; através deste estudo com base em bibliografias foi realizado um levantamento das vulnerabilidades existentes, além da sugestão de definição de políticas

e boas práticas; a disseminação do conhecimento voltado a segurança da informação e também a sugestão de pontos de melhoria para o ambiente corporativo da indústria do Estado do Rio Grande do Sul.

Para tanto, foi elaborado um roteiro de entrevistas no qual foram envolvidos gestores da parte estratégica da empresa e analistas de Tecnologia da Informação para obtenção das informações.

O motivador inicial para este projeto foi levantado através de um trabalho de gestão de riscos realizado na organização, o qual visava garantir a continuidade do negócio da empresa, manter as suas vantagens competitivas e garantir a segurança da informação. No resultado deste trabalho observou-se uma carência voltada à segurança dos dados e informações diante das possibilidades existentes na ferramenta colaborativa do Office 365, na qual as principais vulnerabilidades elencadas foram mencionadas para o compartilhamento facilitado das informações, a possibilidade de grandes cópias para meios externos através dos drives virtuais e, também, o permissionamento descentralizado que pode ser feito pelos usuários da ferramenta, fatores que consequentemente geraram pontos de atenção.

Com a intenção de resguardar a companhia ilustrada neste trabalho de pesquisa, optou-se por não fazer a identificação dela. Desta forma, o artigo apenas mencionará a organização como indústria do Rio Grande do Sul.

Na seção dois deste trabalho, o autor apresenta a fundamentação teórica, preparando o leitor para acompanhar a análise dos resultados descritos no item três. No item quatro, o autor expõe as suas considerações sobre do trabalho, descrevendo as considerações de conclusão e os trabalhos futuros. Ao final, é possível constatar as referências utilizadas.

2 FUNDAMENTOS DA GOVERNANÇA E SEGURANÇA DA INFORMAÇÃO

Serão apresentados nesta seção os conceitos utilizados na construção deste artigo. A partir deles foi desenvolvido o estudo de caso apresentado na seção três.

Fontes (2006) faz um alerta para o progressivo aumento de incidentes relacionados à segurança da informação, principalmente no Brasil. De uma forma natural e sucessiva, as empresas estão cada vez mais expostas a novas formas de ataques, independentemente do porte ou do tipo de negócio.

A inexistência de uma equipe responsável na organização e com um foco pela segurança da informação, a complexidade e o aumento de recursos tecnológicos, são fatores que muitas vezes direcionam os esforços da diretoria e equipe de Tecnologia da Informação de forma reativa em questões relacionadas à segurança da informação.

De acordo com Sêmola (2003), as organizações não devem tratar seus planos de segurança da informação somente em forma de projetos ao invés de internalizar processos para esta finalidade, não perceber a interferência direta da segurança com o negócio, adotar ferramentas pontuais como medida paliativa e tratar as atividades como despesa e não como investimento podem refletir negativamente no negócio da organização.

Na visão de Ferreira (2003), "a segurança da informação protege a informação de diversos tipos de ameaças garantindo a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e das oportunidades".

Diante deste entendimento, é essencial que uma equipe de Tecnologia da Informação de uma companhia tenha um foco na segurança da informação, a fim de resguardar a saúde do negócio, disseminar boas práticas e recomendações, garantindo e preservando as premissas de confidencialidade, disponibilidade e integridade das informações.

Não se pode deixar que arquivos e sistemas de uma organização estejam em situação vulnerável, estando à disposição de pessoas com segundas intenções. Nem sempre os gestores de uma empresa acabam se preocupando com isso, porque muitas vezes eles acreditam que não há probabilidade de uma dessas situações ocorrer em suas empresas. Diante deste olhar, Laureano (2005) destaca a seguinte visão:

> Com a dependência do negócio aos sistemas de informação e o surgimento de novas tecnologias e formas de trabalho, como o comércio eletrônico, as redes virtuais privadas e os funcionários móveis, as empresas começaram a despertar para 10 a necessidade de segurança, uma vez que se tornaram vulneráveis a um número maior de ameaças.

Também nessa percepção ele complementa:

> As redes de computadores, e consequentemente da Internet mudaram as formas como se usam sistemas de informação. As possibilidades e oportunidades de utilização são muito mais amplas do que em sistemas fechados, assim como os riscos à privacidade e à integridade da informação. Portanto, é muito importante que mecanismos de segurança de sistemas de informação sejam projetados de maneira a prevenir acessos não autorizados aos recursos e aos dados desses sistemas.

Desta forma, se faz necessária a busca e análise de informações sobre a saúde da segurança das informações e arquivos hospedados na plataforma do Office 365. Essa ação pode ser considerada proativa, pois até o momento das coletas de informações e análises, não foi relatado ou evidenciado nenhum prejuízo à imagem da empresa, nem mesmo vazamentos ou perda de informações.

A governança pode ser definida por um conjunto de hábitos e atribuições exercidas pelos gestores da administração e gerência estratégica, garantindo que os objetivos sejam alcançados, que os riscos sejam tratados de forma apropriada e que os recursos da empresa sejam utilizados de forma consciente e responsável. (GULDENTOPS, 2003).

Pode-se ainda complementar e descrever a governança como um conjunto de responsabilidades e práticas realizadas pelo conselho administrativo e executivo, na qual um dos objetivos é provisionar o direcionamento estratégico da empresa, para que esse possa garantir que os objetivos sejam atingidos, acompanhando os riscos identificados e determinando que eles sejam conduzidos de maneira adequada; e que a infraestrutura da empresa seja usufruída de forma responsável e eficaz (IGTI, 2006).

Para Albertin (2004), a governança de Tecnologia da Informação procura definir uma estrutura de relações e processos que dirige e controla uma organização a fim de agregar valor ao negócio através do gerenciamento balanceado do risco e do retorno do investimento de Tecnologia da Informação.

A governança de Tecnologia da Informação atua com ênfase em cinco domínios, todos engajados com as premissas dos *stakeholders*, sendo que dois são resultados: Valor

de Tecnologia da Informação e Gerenciamento de Risco; e três são direcionadores: Alinhamento Estratégico, Gerenciamento de Recursos e Medidas de Performance (BOARD BRIEFING ON IT GOVERNANCE, 2º Edição).

Entre os conceitos gerais de governança fundamentados anteriormente, destacam-se os valores voltados aos riscos, pois além do passo importante de identificação deles, o tratamento e o acompanhamento são essenciais para a preservação da saúde da organização.

3 ANÁLISE DO AMBIENTE

Este estudo de foi elaborado no ambiente corporativo da companhia denominada como indústria do Rio Grande do Sul, que está localizada na região sul do país. Ela utiliza e disponbiliza os recursos da ferramenta colaborativa Office 365 para os seus colaboradores internos e externos.

Para isto, foi utilizada metodologia de pesquisa através da revisão bibliográfica de assuntos referentes ao tema, o que oferece um maior aprofundamento do assunto ao estudante, fazendo com que este possa entender a visão consolidada do mundo acadêmico e questionar os novos pontos que trazem fomento à pesquisa.

Tal metodologia classifica-se como qualitativa, onde o autor participa, compreende e interpreta os fatos. Os sujeitos elencados para a pesquisa compõem a equipe de Infraestrutura de TI contendo 4 colaboradores, 6 membros da gestão e também 2 executivos da alta direção.

Logo, percebe-se que a dependência dos recursos tecnológicos aliada a preocupação com a segurança das informações despertada em um trabalho de gestão de riscos, motivou o interesse na realização da pesquisa e obtenção dos dados.

O Office 365 é uma suíte de aplicativos e soluções online que é contratada por assinatura. Ela oferece acesso a serviços e *softwares* construídos em torno da plataforma Microsoft Office. Ela busca atender diversas demandas do ambiente corporativo, oferecendo desde aplicativos para criação de documentos, planilhas e apresentações até

soluções para armazenamento de dados em nuvem e desenvolvimento de portais colaborativos.

Figura 01 – Aplicativos e Serviços do Office 365 (Utilizados pela Empresa e Analisados)

	Disponíveis	Utilizados	Analisados
Word	X	X	
Excel	X	X	
PowerPoint	X	X	
Outlook	X	X	
OneNote	X		
Exchange	X	X	
OneDrive	X	X	X
SharePoint	X	X	X
MicrosoftTeams	X	X	
Yammer	X		

Fonte: Dados da Pesquisa, 2019.

Através da Figura 01 apresentada, foi possível observar todos os aplicativos e serviços disponíveis na suíte do Office 365. A indústria do Rio Grande do Sul optou por não fazer a utilização de todos; os recursos utilizados por ela foram destacados na coluna denominada “utilizados”. Através da análise do ambiente foi possível diagnosticar e compreender quais destes componentes são os que geram o ponto de atenção voltado à segurança da informação, que originaram o estudo. Esses foram listados na coluna denominada “analisados”.

O OneDrive é um serviço de armazenamento de arquivos em nuvem. Através dele é possível armazenar e compartilhar qualquer tipo de arquivo, sendo também possível

definir arquivos e compartilhá-los como modo público, em que qualquer pessoa poderá acessar o conteúdo definido nesta modalidade. O serviço oferece grandes áreas de armazenamento e pode ser contratado de forma customizada e flexível de acordo com as demandas da empresa.

O SharePoint é um serviço que disponibiliza uma plataforma de aplicações Web, ele possibilita a utilização e a criação de portais e intranets empresariais, permite fazer a gestão de conteúdo, gestão documental e também a criação de portais colaborativos, viabiliza a publicação de aplicações web e a criação de fluxos. É uma plataforma bem ampla que pode ser customizada de acordo com as necessidades da empresa, ela possui plena integração com o OneDrive, pois havendo a necessidade de armazenamento de arquivos eles funcionam em conjunto.

3.1 ANÁLISE DOS DADOS

A partir das informações coletadas foi possível compreender a situação atual da indústria que foi o objeto desta pesquisa, para posteriormente propor mudanças e melhorias para a sua estrutura. Além disso, foi possível notar por meio da análise dos dados coletados a ausência de documentação, bem como da participação e do planejamento da equipe de Tecnologia da Informação nos projetos e implementações.

Foi identificado que a implementação da ferramenta Office 365 na organização se realizou por meio de uma empresa terceira que foi contratada para realização deste projeto.

Ademais, foi evidenciado que a empresa contratada efetuou a implementação com pouco envolvimento da equipe interna de Tecnologia da Informação da indústria do Rio Grande do Sul. Esse fato pode ter contribuído para uma implantação de formato padrão, na qual todos os recursos acabaram ficando habilitados para todos usuários, sem considerar a definição de políticas e boas práticas.

Dando seguimento na análise dos dados, constatou-se que todos os utilizadores das ferramentas OneDrive e SharePoint possuem o mesmo tipo de permissionamento

aplicado, diferenciando apenas dos administradores de rede que possuem permissões elevadas e todos privilégios administrativos do portal de administração da ferramenta Office 365.

Em uma análise mais aprofundada da ferramenta OneDrive, foi possível identificar que todas as áreas da empresa fazem a sua utilização. Além disso, também foi constatado que, por haver uma falta de recursos internos para armazenamento de arquivos, as áreas passaram a trabalhar com um ambiente híbrido das pastas dos setores, ou seja, passaram a copiar arquivos novos e migrar os setores existentes do servidor interno de arquivos para as pastas disponíveis no OneDrive. Com isso, passaram a contornar a falta de espaço do servidor interno, mas ao mesmo tempo deixaram vulneráveis as informações copiadas para o OneDrive, porque nela, atualmente, não existe a distinção de permissionamento através de grupos e pastas que existe no servidor interno.

Outra fragilidade encontrada no OneDrive é o fato de que todos usuários podem copiar, excluir e compartilhar todas as pastas e arquivos existentes. Os compartilhamentos, inclusive, podem ser feitos para pessoas de fora da organização, com a opção de compartilhamento público. Isso demonstra certa fragilidade da ferramenta, já que todos podem alterá-la de forma integral.

Já a análise realizada na plataforma do SharePoint também permitiu a identificação de importantes pontos. O primeiro deles foi a possibilidade de todos usuários poderem visualizar e editar todos conteúdos existentes; ainda, todos podem fazer a criação e edição de grupos de permissionamento e distribuição de e-mails. Nesse sentido, foram evidenciados diversos grupos de e-mails criados sem haver um mínimo padrão e organização, fato que dificulta a identificação e administração desta.

Mais um fator de atenção pode ser levantado é o de que todos utilizadores podem tornar o acesso público sem a necessidade de autenticação, aos portais de projetos e intranet existentes, possibilitando que informações sigilosas e importantes possam ser acessadas e manipuladas.

3.2 OPORTUNIDADE DE MELHORIAS

As ferramentas analisadas possibilitam importantes oportunidades de melhorias. Nesse sentido, necessita-se de uma sugestão voltada a uma melhor documentação dos projetos realizados, levando em consideração que não foi encontrado para o projeto do Office 365 nenhuma documentação básica e clara, em que poderia constar desde requisitos básicos do pré-projeto até registros de históricos do andamento e da finalização deste.

Outro avanço que deveria ser aperfeiçoado para ambas as ferramentas é a adoção e criação de grupos e níveis de segurança. Inicialmente, a categorização poderia existir por setores, na qual cada área só teria acesso ao seu conteúdo, exceto em casos pontuais da necessidade de inclusão de um usuário de diferente setor a um tema específico.

Também em cada setor poderiam existir ao menos três níveis de segurança, em que um deles seria de usuários que teriam privilégios mínimos necessários para o desempenho das suas atividades. Já um segundo nível poderia compor pelo menos dois usuários chave por área; esses seriam referência para o permissionamento de pastas e grupos do setor, em que receberiam treinamento e orientações necessárias.

Com isso, não necessitaria da dependência de Tecnologia da Informação para essa atividade. Por fim, ainda seria necessário um terceiro nível para realização de compartilhamentos e publicações, principalmente públicas e com externos, que são casos críticos e delicados. Esse nível poderia contar com a *expertise* e olhar do gestor de cada área para aprovação e consentimento, desta forma elevando o grau de segurança sem perder o dinamismo proposto pela ferramenta.

É indispensável a criação de uma política de utilização, não necessitando ser algo extenso e complexo, constando claramente para o usuário da ferramenta informações sobre o proposito e a sua finalidade, orientações e boas práticas que devem e podem ser seguidas, principalmente voltadas ao compartilhamento de pastas, arquivos e portais.

Para um resguarde e segurança da empresa sobre as informações transferidas do servidor interno de arquivos, cabe uma revisão de tudo que foi arquivado no OneDrive

até o momento, para que se possa validar a conformidade ou a necessidade de retirada ou transferência de alguma informação.

Por fim, a empresa deveria revisitar e possivelmente aperfeiçoar a maneira de como conduz os seus projetos. É indispensável que a equipe de Tecnologia da Informação tenha uma maior participação principalmente em projetos que tenham uma conexão ou que gerem impactos na área. O olhar deste time qualificado aliado a uma metodologia de projetos são capazes de plena qualificação e trazem bons resultados.

4 CONSIDERAÇÕES

Através da realização deste estudo foi possível assegurar e exibir os benefícios da Governança e Gestão da Segurança da Informação, no qual se evidenciou que os resultados de um trabalho de gestão e de tratamento para os riscos identificados são essenciais para uma organização, pois as informações corporativas são um ativo de suma importância para a continuidade dos negócios.

Foram cumpridos todos os objetivos propostos através da metodologia, em que pese que foi realizada a pesquisa bibliográfica profunda sobre o assunto, de forma virtual e física, bem como foi feita a aplicação da pesquisa prática na indústria do Estado do Rio Grande do Sul.

Através disso, tornou-se possível mensurar a importância de realizar uma boa definição do escopo de projetos antes do seu início. Ademais, o envolvimento de pessoas e equipes afetadas direta e indiretamente é indispensável para se evitar problemas futuros, visto que esses possam ocasionar falhas ou comprometer a produtividade dos negócios da organização.

Vale observar os benefícios dessa pesquisa para a empresa, porque ofertou a oportunidade de realizar melhorias em seu ambiente através das sugestões propostas, assim como melhorias para as pessoas envolvidas que, de uma forma ou outra, contribuíram e tiveram a oportunidade de se desenvolver de alguma forma através da troca de informações, além de oportunizar o olhar de pontos de vistas diferentes.

O estudo atentou para a relevância de se possuir processos e projetos documentados, da mesma forma que a importância de possuir definições de políticas e boas práticas aplicadas.

Constatou-se também que a equipe de Tecnologia da Informação, através de suas responsabilidades e conhecimentos, possuí uma atuação muito ampla e relevante para manter o negócio produtivo e garantir o fluxo e andamento das operações.

Como forma de trabalho futuro deseja-se fazer um trabalho mais amplo de diagnóstico e aderência, baseando-se na ISO 27001 que é o padrão e a referência internacional para a gestão da segurança da informação, pois a oportunidade de visitar todos os processos e a estrutura da empresa traria muitas melhorias, confiabilidade e segurança para organização, haja vista que ela teria com este trabalho um apanhado geral de toda a sua estrutura.

REFERÊNCIAS

ALBERTIN, Alberto Luiz. **Administração de Informática. Funções e Fatores Críticos de Sucesso.** 5 ed. São Paulo: Editora Atlas, 2004.

BOARD BRIEFING ON IT GOVERNANCE. Disponível em <http://www.isaca.org/KnowledgeCenter/Research/ResearchDeliverables/Pages/Board-Briefing-on-IT-Governance-2nd-Edition.aspx>. Acessado em 12 jul. 2019.

CAMPOS, A. **Sistemas de Segurança da Informação.** 2 ed. Florianópolis: Visual Books, 2007.

FERREIRA, Fernando Nicolau Freitas**. Segurança da Informação.** Rio de Janeiro: Editora Ciência Moderna Ltda, 2003.

FONTES, Eduardo. **Segurança da Informação: O Usuário Faz a Diferença.** São Paulo: Saraiva, 2006.

GULDENTOPS, Erik. **Board Briefing on IT Governance.** 2003. Disponível em: <https://www.isaca.org/restricted/Documents/26904_Board_Briefing_final.pdf >. Acessado em 06 jul. 2019.

LAUREANO, Marcos Aurelio Pchek. **Gestão de Segurança da Informação.** Disponível em: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20

.pdf>. Acessado em 09 jul. 2019.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: Uma Visão Executiva.** Rio de Janeiro: Elsevier, 2003.

IT GOVERNANCE INSTITUTE. **Information Security Governance: Guidance for Boards of Directors and Executive Management.** 2 ed. The IT Governance Institute, 2006. Disponível em: < https://www.slideshare.net/CristianNascimento/cobit41-portuguese-18008952 > Acessado em 22 jul. 2019.

ITGI. **Information Security Governance: Guidance for Boards of Directors and Executive Management.** 2 ed. Disponível em: <http://www.isaca.org/knowledge-center/research/documents/information-security-govenance-for-board-of-directors-and-executive-management_res_eng_0510.pdf>. Acessado em 04 jul. 2019.