UMA ABORDAGEM PARA GERENCIAMENTO DE RISCOS EM TECNOLOGIA DA INFORMAÇÃO

Adauto Cavalcante Menezes[1], Demair de Sá Ramos[2], Jefferson Gonzaga dos Santos[3], José dos Santos Machado[4], Toniclay Andrade Nogueira[5].

[1]Mestre em Ciência da Computação, Técnico de Tecnologia da Informação do Instituto Federal de Sergipe, adauto.cavalcant@gmail.com; [2]Pós Graduado em Gestão Infraestrutura de Redes, Técnico de Tecnologia da Informação do Instituto Federal de Sergipe, demair.sramos@gmail.com; [3]Especialização em MBA em Governança de T.I, Técnico de Tecnologia da Informação do Instituto Federal de Sergipe, jeffersongonzaga.stos@gmail.com; [4]Mestre em Ciência da Computação, Técnico de Tecnologia da Informação do Instituto Federal de Sergipe, jsmac18@hotmail.com; [5]Mestre em Ciência da Computação, Docente do Instituto Federal de Sergipe, toniclay@globo.com.

Resumo: O objetivo do estudo é evidenciar os principais passos para a identificação, tratamento e monitoramento contínuo dos riscos associados à tecnologia da informação e controles internos, bem como, estudar e apontar soluções preliminares do risco associado ao aspecto de negócio. A discussão teórica parte do tema gerenciamento de riscos em tecnologia da informação aplicado a uma empresa. Os dados foram coletados por meio de uma entrevista com diretor de tecnologia da informação, afim de identificar a sua devida aplicação. Como conclusão, comprovou-se a necessidade da aplicação de boas práticas.

Palavras-chave: Gerenciamento. Risco. Ameaças. Incertezas. Segurança.

Abstract: The objective of the study is to highlight the main steps for the identification, treatment and continuous monitoring of the risks associated with information technology and internal controls, as well as to study and point out preliminary solutions to the risk associated with the business aspect. The theoretical discussion starts with the topic of risk management in information technology applied to a company. The data were collected through an interview with director of information technology, in order to identify its application. As a conclusion, the need to apply good practice has been proven.

Keywords: Management. Risk. Threats. Uncertainties. Safety.

INTRODUÇÃO

Nesta era digital, as organizações usam a informação automatizada, tecnologia da informação para processar as suas informações provendo um melhor suporte ao seu negócio. O gerenciamento de riscos desempenha um papel crítico na proteção de ativos da informação de uma organização. Para que o programa de segurança de tecnologia da informação venha a ter sucesso, torna-se necessário que o gerenciamento de riscos seja eficaz (FERREIRA, ARAÚJO, 2008).

Diante deste contexto, tem-se como objetivo geral estudar e apontar soluções preliminares do gerenciamento de risco associado ao aspecto de negócio. Fontes (2008) afirma que o principal objetivo do gerenciamento de risco de uma organização é proteger a organização e sua capacidade de realizar a sua missão, e não apenas os seus ativos de TI. Portanto, o gerenciamento de risco não deve ser tratado principalmente como uma função técnica realizada pela TI, mas como uma função essencial de gestão da organização.

Segundo Stoneburner, Goguen e Feringa (2019), o risco é o impacto líquido negativo do exercício de uma vulnerabilidade, considerando tanto a probabilidade quanto o impacto da ocorrência. A gestão de riscos é o processo de identificação de riscos, avaliação de riscos, tomada de medidas para reduzir o risco a um nível aceitável.

Diante da crescente concorrência e compe-

titividade das empresas, os negócios estão cada vez mais dependentes da tecnologia da informação. A escolha do tema justifica-se pela necessidade de proteger as informações da corporação de forma confiável, mantê-las sempre disponíveis e sem interrupções. Desta forma o gerenciamento de riscos em tecnologia da informação torna-se essencial para evitar que as falhas venham a causar um impacto negativo na corporação, de forma a prover a continuidade dos negócios.

O presente estudo delimita-se a pesquisar o gerenciamento de riscos em tecnologia da informação aplicado a um órgão público federal, de forma a compreender a importância e necessidade de proteger as informações, prevenir as falhas, evitando que estas se tornem pesadelos ou até verdadeiras catástrofes. O gerenciamento de riscos deve ser trabalhado de forma a prevenir falhas e acidentes, a probabilidade de falhas são minimizadas ao trabalhar de forma antecipada os possíveis problemas.

Para o alcance, o objetivo do presente estudo utilizou-se, como metodologia de pesquisa, a aplicação de um questionário que serviu de base para levantar dados sobre o processo de gerenciamento de riscos em tecnologia da informação a uma empresa de nome XPTO (nome fictício, a mesma não nos autorizou divulgar o verdadeiro nome), bem como, a revisão da literatura sobre gerenciamento de riscos em tecnologia da informação. Em seguida, serão apresentados os resultados dos dados encontrados e a validação das hipóteses/proposições. O artigo é concluído com a resposta à questão de pesquisa, com apresentação das limitações e recomendações para novas pesquisas.

REFERENCIAL TEÓRICO

A informação, independentemente de seu formato, é um ativo importante da organização. Por isso, os ambientes e os equipamentos utilizados para seu processamento, seu armazenamento e sua transmissão devem ser protegidos, pois, a informação tem valor para a organização, uma vez que sem informação, a organização não realiza seu negócio (FONTES, 2008).

Fatores econômicos, ambientais, políticos, tecnológicos, infraestrutura, pessoas e qualidade são alguns dos fatores externos que influenciam a operacionalização do gerenciamento de riscos.

Segundo Stoneburner, Goguen e Feringa (2019), este processo não é exclusivo para o ambiente de TI; na verdade, permeia a tomada de decisões em todas as áreas de nossas vidas, afinal o gestor de uma unidade organizacional deve garantir que a organização possua as capacidades necessárias para o bom desenvolvimento do negócio e que este gestor deve determinar o nível de segurança que os sistemas de TI devem ter com a corporação, diante das atuais ameaças mundiais.

A maioria das organizações tem orçamentos apertados para a segurança de TI, portanto, os gastos com segurança de TI devem ser reavaliados, bem como outras decisões devem ser tomadas pela gestão (STONEBURNER, GOGUEN, FERINGA, 2019).

Uma das razões fundamentais para implementar o gerenciamento de riscos na organização é minimizar o impacto negativo. Um gerenciamento de riscos bem estruturado contribui de forma satisfatória com a administração para identificar adequadamente os recursos de segurança essenciais para a organização (FERREIRA, ARAÚJO, 2008).

Segundo Ferreira e Araújo (2008), a avaliação e análise de riscos são os primeiros passos para a gestão de riscos. Para determinar a probabilidade de um evento, as ameaças existentes que cercam o ambiente de tecnologia da informação devem ser analisadas, bem como as vulnerabilidades potenciais e controles de segurança implementados e disponíveis. Para Stoneburner, Goguen e Feringa (2019), o impacto é o resultado de um dano causado por uma ameaça que explorou uma vulnerabilidade.

Como visto, vários autores abordam o gerenciamento de riscos como uma solução essencial para a organização, a fim de minimizar as perdas e maximizar os lucros. Utilizam de normas e guias para prover a aplicação de boas práticas. Pode-se constatar que o fundamento dos autores parte sempre da série da norma ISO 27000, que é uma norma da organização internacional de normalização, exclusiva para assuntos de tecnologia da informação.

Os autores Ferreira e Araújo (2008) e Stoneburner, Goguen e Feringa (2019) sugerem a abordagem de nove passos para serem seguidos como metodologia de gerenciamento de riscos, sendo eles: caracterização dos sistemas, identificação das ameaças, identificação das vulnerabilidades, análise dos controles de segurança, determinação da probabilidade, análise de impacto, determinação do risco, recomendações dos controles e documentação dos resultados.

Na caracterização dos sistemas, as limitações dos sistemas são identificadas por meio dos recursos e informações que os constituem. Caracterizar um sistema informatizado ajuda na definição do escopo e abrangência, delineia os limites para autorizações e fornece informações essenciais para definir o risco (FERREIRA, ARAÚJO, 2008). A norma NBR ISO/IEC 27005:2005 recomenda que as informações sejam reunidas para que seja possível determinar o ambiente em que ela opera e a relevância desse ambiente para o processo de gestão de riscos de tecnologia da informação.

Identificar riscos em sistemas informatizados requer uma grande compreensão do seu ambiente de processamento e de sua finalidade. Os responsáveis pela condução da avaliação de riscos devem coletar as seguintes informações relacionadas aos sistemas sob análise (FERREIRA, ARAÚJO, 2008).

Stoneburner, Goguen e Feringa (2019) entendem por ameaça a possibilidade de um invasor ou evento inesperado explorar uma vulnerabilidade, considerando esta como uma fraqueza que pode ser acidentalmente utilizada ou intencionalmente explorada e afirma que este passo pretende identificar de forma efetiva as fontes de ameaças e sua formação, destacando as ameaças potenciais que são aplicáveis ao ambiente avaliado.

Segundo Ferreira e Araújo (2008) vulnerabilidade é a falha ou fraqueza no sistema de procedimentos de segurança, projeto, implementação, ou controles internos que poderiam ser exercidos (acidentalmente ou intencionalmente acionado) e resultar em uma violação de segurança ou uma violação da política de segurança do sistema de informação. O objetivo deste passo é desenvolver uma relação das vulnerabilidades do sistema que podem ser exploradas pelas potenciais fontes de ameaça.

A etapa análise dos controles de segurança, tem como objetivo analisar os controles que foram implementados, ou estão previstos para implementação pela organização, para minimizar ou eliminar a probabilidade de uma ameaça ou vulnerabilidade no sistema.

Os controles de segurança incluem a utilização de métodos técnicos e não técnicos. Os controles técnicos são aqueles que são incorporados como hardware, software ou firmware (por exemplo, acesso mecanismos de controle, mecanismos de identificação e autenticação, métodos de criptografia, software de detecção de intrusão). Os controles não-técnicos são controles gerenciais e operacionais, tais como as políticas de segurança, procedimentos operacionais, pessoal, físico e ambiental (FERREIRA, ARAÚJO, 2008).

Para Stoneburner, Goguen e Feringa (2019) as categorias de controle para ambos os métodos podem ser classificadas como preventivas e investigativas; afirma ainda que as preventivas inibem as tentativas de violação às políticas de segurança e incluem mecanismos de controle de acesso, criptografia e autenticação, já as investigativas alerta as violações, ou tentativas, das po-

líticas de segurança e incluem trilhas de auditoria e mecanismos de detecção de intrusos. Uma boa técnica para analisar os controles de segurança, seria o desenvolvimento de checklists de segurança, afinal pode ser muito útil para analisar a eficácia dos controles de segurança utilizados.

Na determinação da probabilidade, Stoneburner, Goguen e Feringa (2019) defendem ser necessário determinar uma classificação geral de ocorrência que uma potencial vulnerabilidade possa ser explorada, fatores como motivação da ameaça, natureza da vulnerabilidade, existência e eficácia dos controles devem ser considerados.

Antes de iniciar uma análise de impacto é necessário ter em mãos as informações que foram levantadas na etapa de caracterização dos sistemas, pois, estes resultados podem determinar o impacto na organização caso os sistemas sejam comprometidos.

A norma NBR ISO/IEC 27005:2008 aborda que a melhor forma para determinar o grau do risco é relacionar em detalhes quais seriam os impactos para a organização, se uma ameaça conseguir explorar uma vulnerabilidade e caso a avaliação de impacto nunca tiver sido realizada, a criticidade dos sistemas pode ser determinada no nível de proteção necessária para manter a confidencialidade, integridade e disponibilidade.

A determinação do risco tem como objetivo avaliar o nível de risco dos sistemas, podendo ser expressado através da probabilidade de ocorrência, do nível de impacto causado pelo sucesso da exploração de uma vulnerabilidade e da eficácia nos controles de segurança. A norma NBR ISO/IEC 31000:2009 atribui que a determinação inclua todos os riscos, estando suas fontes sob o controle da organização ou não, mesmo que as fontes ou causas dos riscos possam não ser evidentes. Além de identificar o que pode acontecer, é necessário considerar possíveis causas e cenários que mostrem quais consequências podem ocorrer; deve-se considerar todas as causas e possíveis consequências.

De acordo com Stoneburner, Goguen e Feringa (2019) na etapa de recomendações dos controles, deve selecionar os controles de segurança que serão utilizados para minimizar os riscos identificados que poderão, se explorados, afetar as operações da organização. O objetivo dos controles que serão recomendados é para reduzir o nível de risco que os sistemas estão expostos até um nível aceitável. Stoneburner, Goguen e Feringa (2019) orientam que os seguintes fatores devem ser considerados e recomendados, a eficácia das opções recomendadas, legislação e regulamentação, a política organizacional, impacto operacional, segurança e confiabilidade.

As recomendações de controle são os resultados do processo de avaliação de risco e contribui para o processo de mitigação de risco, durante o qual a segurança processual e técnica recomendada de controle são avaliados, priorizados e implementados. Nota-se que nem todos os possíveis controles recomendados podem ser aplicados para reduzir a perda.

Uma vez que a avaliação do risco foi concluída (ameaças e vulnerabilidades identificadas, riscos avaliados, e os controles fornecidos recomendados), os resultados devem ser documentados, gerando um relatório de avaliação de risco, que é um relatório de gestão que auxiliará a alta administração com o negócio e em tomadas de decisões.

A redução de riscos envolve priorização, avaliação e implementação dos controles de redução de risco adequados recomendados. Certo de que a eliminação de todos os riscos é normalmente impraticável ou quase impossível, é de responsabilidade da alta administração e dos gerentes do negócio para usar o menor custo e implementar os controles mais adequados para diminuir o risco da organização a um nível aceitável, com o mínimo de impacto negativo sobre os recursos da organização (FERREIRA, ARAÚJO, 2008).

METODOLOGIA DE PESQUISA

A pesquisa utilizou como abordagem metodológica o estudo de caso, estratégia que demanda uma avaliação qualitativa, pois objetiva estudar o processo de gerenciamento de riscos em tecnologia da informação aplicado a uma empresa, uma unidade pública de ensino. Sendo aplicado um questionário dentro do contexto real e sem oferecer ao pesquisador a possibilidade de controle sobre as variáveis (THEÓPHILO & MARTINS, 2009). Além do mais a escolha pode ser justificada, dado que o pesquisador não teve controle sobre os eventos. A participação foi caracterizada como a de observador passivo.

Em termos do contexto, a pesquisa tratou de tema relevante de avaliação de gestão de risco em tecnologia da informação aplicado a uma empresa, sendo possível o relato do caso para a comunidade, especialmente os interessados em continuidade do negócio. O assunto é contemporâneo, pois tem despertado interesse por diversos autores e pesquisadores ao longo da última década. A seleção da unidade de análise foi intencional, a fim de demonstrar a importância da aplicação do processo de gerenciamento de riscos em tecnologia da informação.

O processo de pesquisa foi organizado em quatro fases: pesquisa bibliográfica, coleta de dados, análise das informações primárias e secundárias e avaliação dos dados, que serão comentados a seguir.

Na pesquisa bibliográfica, desenvolveu-se a referência teórica com o objetivo de suportar a análise da base empírica levantada junto ao entrevistado. Este referencial buscou identificar as abordagens sobre o gerenciamento de riscos em tecnologia da informação. Deu-se ênfase aos aspectos de incidentes com origem em falhas. Estudou-se também a parte da literatura envolvendo competências e seu desenvolvimento.

Após a elaboração do referencial teórico, por meio de pesquisa bibliográfica, foi realizada a entrevista com diretor de tecnologia da informação, com o objetivo de entender a gestão de riscos em tecnologia da informação aplicada na empresa. Na avaliação dos dados será feita uma análise do conceito aplicado na empresa em confronto com o encontrado na revisão de literatura, concluindo assim o artigo e abrindo novos rumos à pesquisa no tema abordado.

AVALIAÇÃO

Pode-se inferir que a empresa XPTO não possui um processo formatado de gerenciamento de riscos em tecnologia da informação. Isso fica claro quando o entrevistado diz, que em dois anos na direção de tecnologia da informação da XPTO, houve um investimento de oito milhões, para estruturar, prover novas tecnologias à comunidade e aos funcionários. O entrevistado reforça que até o momento não tem processo para tratamento de incidentes, porém, este será o seu próximo passo. Ferreira e Araújo (2008) afirmam que o sistema de gestão em tecnologia da informação é o resultado da aplicação planejada de objetivos, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas que, de forma conjunta, definem como são reduzidos os riscos para a tecnologia da informação.

O entrevistado concorda que o processo de tratamento de incidentes de tecnologia da informação gera informações que possibilitam um melhor planejamento para a proteção do ambiente de tecnologia, afirmando que o tratamento de incidentes é essencial para a contingência das informações, bem como, para a recuperação de desastres. A norma NBR ISO\IEC 27005:2008 enfatiza a necessidade do tratamento do risco, abordando as diretrizes a serem seguidas.

Quando indagado a respeito da existência de um plano de continuidade de negócio para ser seguido quando da ocorrência de um desastre que indisponibilize recursos de informação, o entrevistado informou que apesar de não ter formatado um plano de gerenciamento de riscos, possui

uma política de backup ativa, o que assegura as informações no caso acima citado. Fontes (2008) defende que o plano de contingência seja elaborado para situações onde exista perda de recursos, e que esses recursos possam ser recuperados de forma menos traumática para a organização.

Recomenda-se que exista um cronograma específico para avaliar e mitigar os riscos da organização, o processo realizado periodicamente deve ser flexível para permitir alterações, devido às grandes mudanças nos sistemas de tecnologia da informação e em seu ambiente de processamento.

Um programa de gestão de riscos bem sucedido conta com o comprometimento da alta administração, o total apoio e participação da equipe de tecnologia da informação, a competência da equipe de avaliação de risco, que deve ter os conhecimentos necessários para aplicar a metodologia de avaliação de risco para o negócio, identificar os riscos da organização, fornecer soluções a baixo custo que atendam as necessidades da organização, a consciência e a cooperação dos colaboradores da organização, que deve seguir os procedimentos e cumprir com os controles implementados para manter a tecnologia da informação de sua organização (STONEBURNER, GOGUEN, FERINGA, 2019).

O entrevistado utilizará como uma das bases para elaboração do seu processo de gerenciamento de risco, as recomendações aqui abordadas.

As organizações, em sua maioria, estão sujeitas a mudanças; a rede poderá estar em contínuo crescimento, seus componentes alterados, e suas aplicações substituídas ou atualizadas por versões mais recentes. Além disso, mudança de pessoal poderá ocorrer e as políticas de segurança são susceptíveis de mudar ao longo do tempo. Estas mudanças significam que novos riscos virão à tona e os riscos previamente mitigados pode novamente tornar-se uma preocupação, dessa forma o processo de gerenciamento de risco deve esta em frequente atualização.

CONSIDERAÇÕES FINAIS

O estudo teve como objetivo evidenciar os principais passos para a identificação, tratamento e monitoramento contínuo dos riscos associados à tecnologia da informação e controles internos, bem como, estudar e apontar soluções preliminares do risco associado ao aspecto de negócio. Os resultados encontrados por meio de revisão bibliográfica, coleta de dados, análise das informações primárias e secundárias e avaliação dos dados indicam que a empresa XPTO não possui um processo de gerenciamento de riscos formatado.

Os resultados, de certa forma, convergem com a literatura sobre o tema, pois, segundo a NBR ISO/IEC 31000:2009, convém que as organizações visem um nível de desempenho apropriado de sua estrutura da gestão de riscos em consonância com a criticidade das decisões a serem tomadas. Para Ferreira e Araújo (2008), a avaliação e análise de riscos são os primeiros passos para a gestão de riscos, pois, para determinar a probabilidade de um evento, as ameaças existentes que cercam o ambiente de tecnologia da informação devem ser analisadas, bem como as vulnerabilidades potenciais e controles de segurança implementados e disponíveis.

A norma NBR ISO/IEC 17799:2005 recomenda que as avaliações de riscos identifiquem, quantifiquem e priorizem os riscos com base em critérios para aceitação dos riscos e dos objetivos relevantes para a organização de forma que os resultados orientem e determinem as ações de gestão apropriadas e as prioridades para o gerenciamento dos riscos de tecnologia da informação, e para a implementação dos controles selecionados, de maneira a proteger contra estes riscos.

Ainda de acordo com a norma NBR/IEC 17799:2005 os sistemas de informação podem ser alvos de ameaças graves que podem ter efeitos adversos sobre as operações de organização, indivíduos ou outras organizações exploram por vulnerabilidades conhecidas e desconhecidas

que comprometem a confidencialidade, a integridade ou a disponibilidade das informações sendo processadas, armazenadas ou transmitidas por sistemas de comunicação de dados. Ameaças à informação se dão por ataques propositais, desastres ambientais e até erros humanos, o que pode resultar em um grande prejuízo para os interesses da organização.

Portanto, pode-se inferir após a conclusão da pesquisa, que é recomendável que os líderes e gestores em todos os níveis entendam suas responsabilidades, sejam os responsáveis pela gestão de riscos em tecnologia da informação. O Gerenciamento de Risco relacionado com o funcionamento e utilização dos sistemas de informação é apenas um dos muitos componentes do risco organizacional que os líderes e executivos tratam como parte de suas responsabilidades na gestão do negócio.

A gestão eficaz de riscos exige que as organizações operem em ambientes altamente complexos, interligados, diretamente conectados, com um legado de sistemas de informações para proteger a integridade da informação, de forma a cumprir suas missões e conduzir funções importantes no negócio.

As inferências acima descritas devem ser analisadas dentro do seu contexto, considerando algumas limitações do estudo. Os resultados não são conclusivos visto que o gerenciamento de riscos em tecnologia da informação, como gerenciamento de riscos de modo geral, não é uma ciência exata.

Ele reúne as melhores práticas coletivas dentro das organizações, responsáveis pelo planejamento estratégico, supervisão, gerenciamento e rotina diária de operações, provendo melhores resultados à tecnologia da informação, necessários e suficientes para proteger adequadamente as missões e funções do negócio na organização.

O propósito do presente trabalho foi proporcionar novas discussões sobre o tema gerenciamento de riscos em tecnologia da informação, sob a ótica de uma empresa.

Percebeu-se que há possibilidade de aprofundamento sobre o tema, pois, como visto não se trata de uma ciência exata. Uma proposta para estudos futuros é a realização de pesquisa em uma organização que aplique rigorosamente o gerenciamento de riscos em segurança de informação, a fim de validar se os resultados condizem com a literatura, de forma a garantir maior robustez à discussão.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 17799. Tecnologia da informação – Técnicas de segurança – Código de prática para gestão da tecnologia da informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27005. Gestão de risco de tecnologia da informação. Rio de Janeiro, 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 31000. Gestão de riscos – Princípios e diretrizes. Rio de Janeiro, 2009.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Marcio Tadeu, Política de Tecnologia da informação: Guia Prático Para Elaboração e Implementação. Rio de Janeiro: Ciência Moderna, 2008.

FONTES, Edison. Praticando a Tecnologia da informação. Rio de Janeiro: Brasport, 2008.

STONEBURNER, G.; GOGUEN, A.; FERINGA, A. Risk Management Framework for

Information Systems and Organizations. Disponível em: < https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf > Acesso em: 10 de fev. 2019.

THEÓPHILO, C. R., & Martins, G. A. Metodologia da Investigação Científica para Ciências Sociais Aplicadas. São Paulo: Editora Atlas S.A, 2009.