



Segurança da informação em instituições de ensino

Marcela Mayara Barbosa Fernandes, Allysson Steve Mota Lacerda

Introdução

A informação tornou-se o ativo mais valioso de toda e qualquer instituição. Sendo considerada com tanta relevância para a manutenção e continuidade da rotina de atividades, torna-se necessária cautela na manipulação da mesma. Mesmo que de maneira silenciosa os sistemas de informações e suas redes de computadores apresentam-se diante de uma série de ameaças, sendo que, algumas vezes, estas ameaças podem resultar em sérios prejuízos. Mesmo se tratando de uma instituição de ensino, a universidade deve ser considerada como uma organização, uma vez que se trata de um ambiente com características pertinentes a competitividade e que passa por mudanças contínuas, mesmo essa não sendo a principal ou a melhor definição para o termo organização. Todo tipo de organização parte do estudo das informações que detém para alcançar a qualidade, a evolução, a boa gestão, automatização dos seus processos, e ofertar demandas maiores de serviços, caso faça parte da sua missão. Desta forma, a eficaz Governança da Tecnologia da Informação (GTI) se faz tão necessária nesse ambiente.

Já a Segurança da Informação, segundo Coelho e Araújo (2014), é uma ação ou medida para resguardo das informações, levando-se em consideração os variados tipos de ameaças que ronda as organizações. Isso garante a estabilidade do prosseguimento de qualquer negócio de maneira tal que os riscos sejam minimizados, em contra partida aos investimentos e oportunidades de negócios, que devem ser crescentes.

Material e métodos

A. TI em instituições de ensino

Instituições de ensino geralmente possuem redes com grande quantidade de usuários e estações de trabalho conectadas. Essas entidades comumente possuem a gerência de TI centralizadas em um setor. Em caso da instituição possuir um ou mais campi, a administração dos controles de segurança é efetuada de maneira independente. Desta maneira, cada campi ou unidade da instituição fica responsável por sua rede. Fazendo com que assim seja extinta a existência de padrões ou regras dominantes para o todo. Poucas instituições de ensino são estruturadas na área de segurança da informação. Além disso, a implantação de segurança da informação nesses espaços é mais difícil. Não há um setor ou pessoa responsável pela segurança da informação e nem mesmo a preocupação com a importância que essa área tem ou deveria ter dentro de um ambiente acadêmico.

O cenário desse tipo de rede também é caracterizado por pouca demanda de funcionários dedicados à segurança da informação. E isso acaba forçando que a atividade de zeladoria dessa área acabe sendo terceirizada ou que em alguns casos, os cuidados com GTI e com a Segurança da Informação seja exercida pelo Diretor de TI ou Gerente de TI/Redes, aumentando assim o volume de trabalho e responsabilidade do mesmo.

B. Políticas de segurança em TI em instituições de ensino

É reconhecido que não há planejamento ou documentação formal a respeito de Políticas de Segurança da Informação (PSI). Sendo este fator extremamente importante no sucesso dos serviços empreendidos e prestados por Instituições de Ensino.

Muitas instituições têm dificuldade de entender a importância da segurança da informação. Muitos órgãos começam a pensar na implantação de medidas de segurança após terem passado por algum tipo de incidente de segurança, que lhes tenha causado algum dano.

Instituições de ensino são locais com elevado número de pessoas, dados, informações e conhecimento em trânsito. Existe nesse espaço aparatos de TI para oferecer no mínimo a inclusão digital desses indivíduos. E é desejável que toda instituição de ensino ofereça aos seus colaboradores, professores, alunos ou demais cidadãos um serviço de TI bem estruturado e seguro. Para se obter esse resultado o uso da governança da TI e normas de segurança como a ISO 27001 devem ser adotadas.



Devido à ocorrência de problemas relacionados à segurança da informação, problemas esses como pragas, phishing, engenharia social, worm, bot, envio de spam, ataques de negação de serviço e qualquer atividade maliciosa, incluindo ser utilizada para invadir outras máquinas, nota-se a necessidade da sugestão de uma modelo de segurança em TI em instituições de ensino.

C. Governança de TI

A governança de TI e normas de segurança da informação são capazes de orquestrar e assegurar dados e informações em qualquer instituição. Para tanto, é necessário que os métodos e técnicas adequadas a cada realidade sejam implantados. Através da adoção de metodologias de Governança da TI torna-se possível gerenciar riscos, possibilitar mais segurança aos usuários que fazem uso desse aparato tecnológico, seguir padrões de normatização visando uma maior clareza das operações em execução ou serviços disponibilizados, entre outras vantagens.

Resultados

A. Análise da pesquisa bibliográfica

É notório o destaque que uma estrutura de TI bem fomentada desde a sua base de infraestrutura até a capacitação e conhecimento do pessoal que irá implantar esse serviço demonstra eficiência, eficácia e padronização. E ainda deve-se levar em consideração a redução de gastos financeiros e com mão de obra contínua, tanto na implantação quanto na manutenção dessas estruturas e serviços, que se ganha ao aplicar a governança.

Há muito que se ganhar com adesão adequada da segurança da informação, segundo a maneira como ela se apresenta na norma ISO 27001. Essa ação de proteção minimiza riscos de ataques que venham ameaçar a integridade da informação e da estrutura que a armazena, potencializa os retornos esperados e dá mais confiabilidade a TI. Confiabilidade essa que aumenta até a comodidade que o usuário terá ao fazer uso da TI. A área de tecnologia bem estruturada é um fator muito importante na conversão de produtividade em resultados positivos.

Conclusão

É perceptível o impacto que pode ter uma instituição de ensino passando pela linha de criação, manutenção e continuidade deste tipo de conhecimento e proposta causando nos envolvidos nesse processo um bom resultado, assim como os resultados que os demais usufruíram como coleta de frutos. Além de demonstrar uma lealdade aos princípios ensinados e exemplificados, na instituição, a relevância usufruir de padrões e normas voltadas para a TI. É importante ressaltar que é desejável a aplicação desta proposta em todos os processos e setores da instituição.

Sabendo da grandeza e utilidade da governança da TI aplicando a norma de segurança ISO 27001 e após verificar a ausência predominante dessas tecnologias em alguns laboratórios de informática do CCET, sugere-se que seja proposto um modelo de melhorias em governança e da ISO 27001 nesse ambiente.

Referências

- [1] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2005: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005. 120p.
- [2] FERNANDES, A. A.; ABREU, V. F. Implantando a Governança de TI: Da Estratégia à Gestão dos Processos e Serviços. 2ª. ed., Rio de Janeiro, Brasport, 2008. 444p
- [3] MORAES, E. A. P.; MARIANO, S. R. H. Uma Revisão dos Modelos de Gestão em TI. IV Congresso Nacional de Excelência em Gestão – CNEG, 2008, Niterói. Anais... Niterói: CNEG, jul.2008. 19p.