Nível de maturidade em Segurança da Informação: Uma pesquisa voltada a mitigação de riscos em razão do desconhecimento dos usuários de TI.

Amarildo Maia Rolim[1]

[1]Secretaria de Tecnologia da Informação - Universidade Federal do Ceará (UFC)

Fortaleza – CE – Brazil

amarildo.rolim@sti.ufc.br

Abstract

What is perceived today is that despite the systematization in the creation of information security procedures, the insecure behavior of the servers is related as a potential risk to break these procedures, while it reponses the server itself for this failure. In turn, this unsafe behavior can be caused by lack of knowledge and not by malicious action. Therefore, what was sought with this work was through a research, to identify the information security risk factors aimed at the understanding of the work situation, recommending at the end that the results would subsidize a Program of Awareness and Training in Information Security Offered to the institution's servers.

Resumo

O que se percebe hoje é que apesar da sistematização na criação de procedimentos de segurança da informação, o comportamento inseguro dos servidores encontra-se relacionado como um risco em potencial para quebra desses procedimentos, ao passo que responsabiliza o próprio servidor por essa falha. Por sua vez, esse comportamento inseguro pode ser causado pela falta de conhecimento e não por uma ação mal intencionada. Portanto, o que se buscou com esse trabalho foi através de uma pesquisa, identificar os fatores de risco da segurança da informação voltados para a compreensão da situação de trabalho, recomendando ao final que os resultados subsidiassem um Programa de Conscientização e Capacitação em Segurança da Informação ofertado aos servidores da instituição.

1. Introdução

O Governo Federal desenvolve hoje projetos para coordenar a atividade de Segurança de Infraestruturas Críticas, definida como “as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, ou à segurança nacional”. (CANONGIA, 2009, p. 08).

Considerada hoje o maior ativo de qualquer instituição governamental ou empresa privada, a informação deve ser protegida, a tarefa de protegê-la não é simples devido ao grande número de ameaças existentes nas mais diversas áreas, e o desconhecimento do ser humano pode ser uma das maiores vulnerabilidades. Assim, precisamos entender os conceitos que envolvem a relação do homem com seu ambiente de trabalho e os riscos à segurança da informação. Estudos técnicos sobre a Segurança

da Informação realizados por especialistas de diferentes órgãos da Administração Pública Federal comprovam a importância do resultado desta pesquisa ao citar entre as maiores preocupações e recomendações a identificação das interdependências entre os ativos de informação e as pessoas que a eles têm acesso. Ficando então evidenciada a necessidade de se estudar o comportamento dessas pessoas.

Em síntese, considerando-se o pressuposto de que o fator humano e suas relações com as atividades diárias realizadas nos ambientes de tecnologia da informação (TI) podem comprometer a segurança da informação, a pesquisa ora apresentada partiu então das seguintes hipóteses:

1. Existe risco a segurança da informação causado pelo comportamento inseguro dos usuários de TI da UFC;
2. Os comportamentos inseguros são ocasionados pela falta de conhecimento e de conscientização sobre segurança da informação;

A Universidade Federal do Ceará, sediada em Fortaleza, capital do estado, é um braço do sistema do Ensino Superior do Ceará e sua atuação tem por base todo o território cearense, de forma a atender às diferentes escalas de exigências da sociedade. De acordo com o último Anuário Estatístico que tem com referencia o ano de 2016, a UFC possui hoje aproximadamente 2.090 docentes, 3.416 servidores técnicos administrativos e um quadro de pessoal terceirizado que de alguma forma possuem acesso a esses ativos. Desse contexto, buscou-se identificar qual o nível de maturidade dos nossos usuários sobre o tema Segurança da Informação e sua relação com as atividades diárias que podem se transformar em um potencial risco a segurança da informação.

Entende-se que a informação é considerada hoje como indispensável à UFC, vários são os problemas decorrentes da falta de proteção dos ativos de informação. A própria destruição ou alteração dessas informações, a divulgação de informações sigilosas ou mesmo a perda da credibilidade, são alguns dos danos que podem ser causados pela falta de conhecimento de um usuário ao tratar com os ativos de informação. Para Fernandes (2010) um risco de segurança é um evento possível e potencialmente danoso a uma organização, ou seja, um evento com possibilidades de se efetivar, apresentando impacto negativo para a organização. O que comprova a necessidade de manter o controle dos riscos aos quais os ativos estão submetidos.

Deveras, segurança da informação é a garantia que, dentro da instituição, as informações são protegidas para manutenção da sua:

a. Confidencialidade - significa preservar restrições de acesso e divulgação, incluindo os meios para proteger a privacidade e as informações confidenciais;

b. Integridade - significa proteção contra modificação ou destruição inadequada da informação e inclui a garantia de não-repúdio e autenticidade para as informações;

c. Disponibilidade - significa garantir o acesso oportuno e de confiança e o uso adequado da informação.

Portanto, a informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e consequentemente necessita ser adequadamente protegida.

O principal conceito relacionado a essa abordagem é o de Competências para Ação, onde a competência é a experiência constituída antes da ação, que é articulada com o objetivo de sua realização ou o conhecimento necessário para a realização de uma ação, assim como a habilidade utilizada para agir.

Para Marciano (2006), discutir sobre o fator humano como elemento base para se pensar um novo conceito de segurança da informação se coloca como fundamental para efetivação das políticas de segurança da organização.

2.Metodologia

Para efeito deste trabalho, estabeleceu-se um cenário real com a utilização de dados relativos ao comportamento dos usuários de TI na UFC em suas atividades diárias, em busca da mensuração do nível de conhecimento sobre o tema segurança da informação. Dessa forma, foram identificados:

a) os principais riscos envolvidos;

b) os intervalos de classificação dos resultados para priorização das ações.

c) as necessidades de capacitação dos nossos usuários;

Como descrito por Ganga (2012), uma das maneiras de se obter informações sobre uma determinada população é coletar dados sobre os seus elementos, através da utilização do método Survey, uma vez que a pesquisa de avaliação ou Survey coleta informações somente de uma parte da população.

Assim, o questionário da pesquisa foi elaborado com 25 perguntas seguindo os seguintes temas:

a. política de Segurança da Informação e Comunicações (POSIC) da UFC;
b. boas práticas de Segurança da Informação;
c. papeis e responsabilidades do setor;
d. controle de acesso a área física do setor;
e. classificação das informações;
f. registro do acesso às informações;
g. descartes das informações;
h. armazenamento de informações e backup;
i. uso das estações de trabalho;
j. quanto à utilização de senhas de acesso;
k. utilização de anti-vírus atualizado;
l. softwares devidamente licenciados para uso pela UFC;
m. uso de dispositivos pessoais para manipular informações da UFC;
n. acesso a rede sem-fio na UFC;
o. uso do e-mail (Pessoal e Institucional).

3.Resultados

Para se atingir o objetivo geral do trabalho, foram respondidos 114 questionários de um total de 200 convites de participação, ao final foram identificados riscos em potencial a segurança da informação e comprovaram a necessidade de efetivação de um programa de capacitação e conscientização no que se refere a segurança da informação.

Em seguida foi elaborado um documento com alguns riscos encontrados e as respectivas ações necessárias para a mitigação desses riscos e enviado para todos os participantes.

Dentre os resultados encontrados, se destacaram:

a. apesar de aprovada em 2013, a maior parte dos usuários (95) não conhecem a POSIC. Sendo necessária uma ampla divulgação de seu conteúdo;
b. quanto ao conhecimento de boas praticas em SI o resultado demonstra que apesar da metade dos nossos participantes (57) afirmarem conhecer boas práticas em segurança, temos um mesmo quantitativo que desconhece e necessita de capacitação;
c. no que diz respeito ao backup, o resultado demonstra uma necessidade "URGENTE" de se praticar a realização do procedimento de backup;
d. contas são compartilhadas nas estações de trabalho impossibilitando assim a rastreabilidade dos acessos em um processo de auditoria;
e. senhas são compartilhadas. O compartilhamento de senhas é um dos mais graves problemas em Segurança da Informação, a senha é PESSOAL e jamais deve ser compartilhada;

4. Conclusão

Ao final, chegou-se a conclusão com o estudo realizado, que o grande desafio é a melhoraria das percepções, atitudes e capacidades técnicas dos usuários de TI da instituição no que concerne ao valor estratégico da informação, diminuindo assim os riscos envolvidos e deixando evidente a necessidade de se trabalhar através de um processo contínuo e evolutivo o aprimoramento e refinamento dos conhecimentos acerca de segurança da informação. Assim, os resultados podem ser utilizados na elaboração de um Programa de Conscientização e Capacitação em Segurança da informação, o que demonstra o sucesso na realização da pesquisa.

Referencias

Canongia Claudia; Gonçalves Admilson Júnior; Mandarino Raphael. GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA; Guia de Referência Para a Segurança Das Infraestruturas Críticas da Informação. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic>. Acesso em: Agosto de 2014.

FERNANDES, Jorge H. C (org.). Gestão da segurança da informação e comunicações. Volume 1. Brasília: Faculdade de Ciência da Informação, 2010. 113 p. ISBN 978-85-88130-08-1.

GANGA, G. M. D. Trabalho de Conclusão de Curso (TCC) na Engenharia de Produção: uma guia prático de conteúdo e forma. São Paulo: Atlas, 2012. GARVIN, David A. Gerenciando a qualidade . Rio de Janeiro: Qualitym a rk, 1992.

MARCIANO, LIMA-MARQUES, M. O enfoque social da segurança da informação. Ciência da Informação, Ci. Inf. vol.35 no.3 Brasília Sept./Dec. 2006.

Universidade Federal do Ceará. Anuário estatístico da UFC 2017 - Base 2016. Fortaleza. Dezembro 2016.