



II Simposio Internacional de Gestao de Projetos (II Singep)

Simposio Internacional de Inovacao e Sustentabilidade (I S2IS)

FATORES CRITICOS DE SUCESSO EM SEGURANCA DA INFORMACAO EM UM ORGAO DA ADMINISTRACAO PUBLICA FEDERAL

Autoria: Heitor Luiz Murat de Meirelles Quintella,
Marcelo Pereira de Oliveira Branco

RESUMO

Este artigo buscou identificar os Fatores Críticos de Sucesso (FCS) para a implantação de uma Política de Segurança da Informação (PSI) em um órgão da Administração Pública Federal. Apesar de as “melhores práticas” em segurança da informação encontrarem-se normatizadas através da família de normas ISO/IEC 27000 (2005), os FCS variam de uma instituição para outra. O objetivo foi disponibilizar informações a um órgão da Administração Pública Federal que possam subsidiar o projeto de implantação de uma PSI e sua sustentabilidade. A pesquisa está baseada nos estudos de Rockart (1979) sobre as dimensões dos FCS. A elaboração dos FCS foi baseada nos prognósticos de Porter (1986), deduzidos dos estágios do ciclo de vida dos produtos, os quais foram parcialmente validados por um questionário estruturado aplicado aos gestores e demais servidores do órgão da APF estudado, através do teste Kolmogorov-Smirnov. A metodologia utilizada foi baseada no método hipotético-dedutivo de Popper e os resultados encontrados apontaram os FCS para a implantação da PSI.

Palavras-chave: Fatores Críticos de Sucesso, Ciclo de Vida do Produto; Segurança da Informação.

ABSTRACT

This paper sought to identify the Critical Success Factors (CSF) for the implementation of an Information Security Policy (ISP) in an organ of the Federal Public Administration (FPA). Although the "best practices" in information security find themselves legislated through the family of ISO / IEC 27000 (2005), the CSF vary from one institution to another. The objective was to provide information to an agency of the Federal Public Administration in order to support the effective implementation of a ISP and its sustainability. The research is based on Rockart's (1979) studies on the dimensions of the critical success factors. The development of CSF was based on Porter's (1986) predictions, deduced from the stages of the life cycle of the products, which were partially validated by a structured questionnaire applied to managers and other staff of the FPA agency studied, using the Kolmogorov-Smirnov test. The methodology used was based on the hypothetical-deductive method of Popper. The obtained results indicated the CSF for the implementation of ISP.

Keywords: Critical Success Factors, Life Cycle of the Products, Information Security.



II Simpósio Internacional de Gestão de Projetos (II Singep)

Simpósio Internacional de Inovação e Sustentabilidade (I S2IS)

1. INTRODUÇÃO

“A sociedade da informação retrata a crescente importância que a informação, o conhecimento e as inovações tecnológicas assumem na contemporaneidade” (ARAÚJO; ROCHA, 2009).

A informação é um ativo cada vez mais importante para os negócios de uma organização. A proteção eficaz da informação organizacional tornou-se prioritária (QUINTELLA; MELLO, 2008).

Os órgãos e entidades governamentais são organizações complexas e com amplo alcance de suas atividades, lidando com informações importantes, para a prestação de serviço público ao cidadão, e também para a tomada de decisões estratégicas de Estado (TROMPOWSKY, 2010).

A segurança da informação diz respeito à proteção da informação contra ameaças que possam valer-se das vulnerabilidades deste ativo, preservando-o em suas propriedades fundamentais: disponibilidade, integridade, confidencialidade e autenticidade (ABNT, 2005).

Segundo Snee (2007), pessoas são vistas como a base fundamental para qualquer mudança organizacional. Ou seja, sem o devido apoio, apenas uma norma para guiar o processo de introdução de segurança da informação não é suficiente. Devem-se considerar as características críticas dos usuários, pois eles serão responsáveis pela adesão e sustentabilidade da Política de Segurança da Informação e melhorias advindas da mesma.

O interesse pela gestão da segurança da informação vem aumentando proporcionalmente ao surgimento de novas ameaças advindas de diferentes meios, sejam elas humanas ou tecnológicas. Este interesse pode ser observado através de mudanças visíveis no cenário organizacional, onde se percebe maior preocupação sobre a necessidade de investir em segurança da informação. A disseminação e união dos principais padrões e normas em uma única série de normas, ISO/IEC 27000, também corroboram nesse sentido (OLIVEIRA; NUNES; ELLWANGER, 2009).

Segundo a norma brasileira ABNT NBR ISO 27002 (2005), Código de Prática para a Gestão da Segurança da Informação, os sistemas e redes de informação das organizações estão cada vez mais expostos a uma diversidade de ameaças.

De acordo com a última pesquisa GISS (Global Information Security Survey), elaborada a partir de entrevistas com 1,6 mil executivos em 61 países diferentes, 61% das organizações afirmam estarem preocupadas em proteger sua reputação e sua marca, e de fato as empresas estão adotando uma postura proativa, onde 46% indicaram que seus investimentos em segurança da informação aumentaram, e afirmam que 91% dessas organizações possuem uma política de segurança documentada, demonstrando a preocupação com a segurança da informação (Ernst & Young, 2010).

É importante observar que segurança da informação não se limita somente ao âmbito da Tecnologia da Informação, pois a segurança oferecida por recursos tecnológicos não provê toda a demanda que este ativo necessita, conforme a norma ABNT NBR ISO/IEC 27002 (2005).

A gestão de riscos de segurança da informação encontra-se normatizada através da família de normas técnicas ISO/IEC 27000 (2005), que dizem respeito à proteção de ativos de informações valiosas através da segurança da informação, particularmente do uso de Sistemas de Informação e Gestão de Segurança.



II Simposio Internacional de Gestao de Projetos (II Singep) Simposio Internacional de Inovacao e Sustentabilidade (I S2IS)

A norma ISO/IEC 27002, código de prática para a gestão de segurança da informação, tem correspondência direta com padrões nacionais de vários países. Sendo identificada no Brasil como ABNT NBR ISO/IEC 27002 a partir de 2007, anteriormente identificada como ABNT NBR ISO/IEC 17799 (2005).

Sendo assim, existe documentado um grupo completo de controles contendo as melhores práticas para segurança da informação.

Na verdade, se tais controles existem normatizados e dentre os quais se encontra a Política de Segurança da Informação, por que tão poucos órgãos a possuem implantada?

De acordo com a norma ABNT ISO/IEC 27002 (2005), a experiência tem mostrado que existem fatores críticos de sucesso para a efetiva implantação da segurança da informação dentro de uma organização.

Os Fatores Críticos de Sucesso (FCS), de acordo com Rockart (1979), sustentam a realização das metas organizacionais, principalmente nas gerências em que um bom desempenho é necessário para a realização de tais metas, assegurando um desempenho competitivo de sucesso (RODRIGUES, 2005).

1.1. SEGURANÇA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA FEDERAL

Proteção adequada da informação pode ser mais facilmente gerida se forem usadas as “melhores práticas”, que são um conjunto de procedimentos constituídos por padrões e recomendações de institutos de tecnologia (ABNT, 2005), uma vez que provaram sua eficácia através da utilização, e por isso são consideradas essenciais, praticamente em qualquer contexto (ABNT, 2005).

Muitas instituições ainda não se deram conta do problema ou não conseguiram implantar tais práticas, e com isso expõem-se a um risco incalculável. Sobretudo àquelas mais dependentes dos recursos de Tecnologia da Informação (TI).

O Acórdão 2.308/2010 do Tribunal de Contas da União, Ata 33, referente à avaliação da governança de tecnologia da informação na Administração Pública Federal (APF), onde são constatadas precariedades e oportunidades de melhoria, determinações, recomendações e comunicações. Dentre as precariedades está a segurança da informação.

A pesquisa foi feita com trezentos órgãos públicos e as conclusões são do próprio TCU: mais da metade das instituições produz software de forma amadora; mais de 60% não tem política e estratégia para sua informática e segurança de informação; 74% não têm as bases de um processo de gestão de ciclo de vida de informação inventariado; 75% não gerenciam incidentes de segurança de informação; 83% não tem ideia dos riscos a que a informação sob sua responsabilidade está sujeita, 89% não classifica informação para o negócio, o que significa que a instituição está sob provável caos informacional e quase 100% não tem um plano de continuidade de negócio em vigor, o que significa que em caso de desastre, o público alvo e dependente de tais informações pode ficar sem o serviço por um período de tempo não estimado (BRASIL, 2010).

A figura 1 resume os principais resultados desse levantamento.



II Simpósio Internacional de Gestão de Projetos (II Singep) Simpósio Internacional de Inovação e Sustentabilidade (I S2IS)

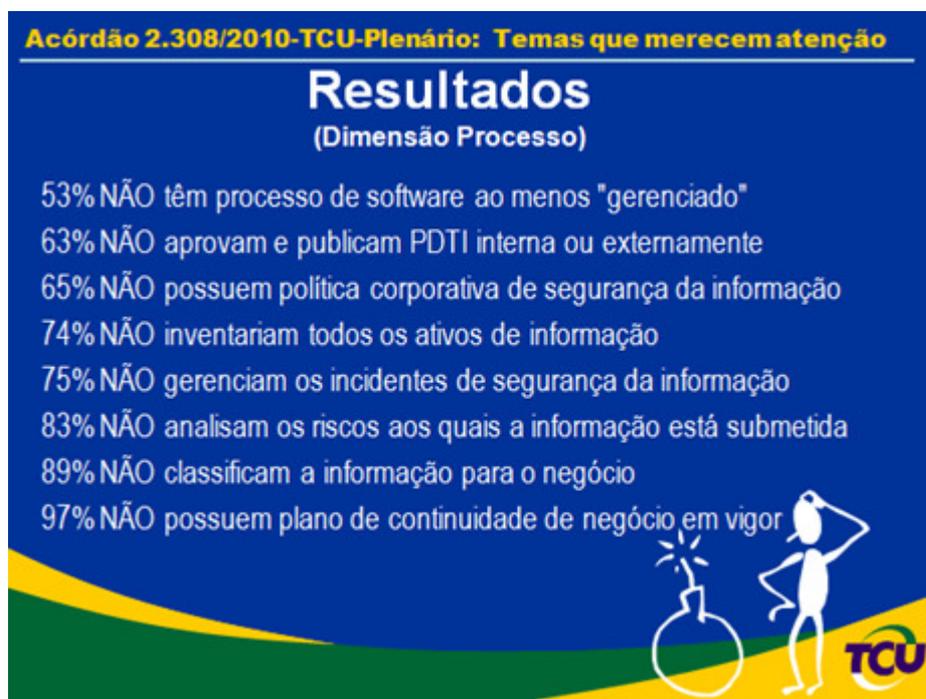


Figura 1 - Avaliação da governança de tecnologia da informação na APF
Fonte: Relatório de Levantamento TC 000.390/2010-0

A presente pesquisa foi realizada em um órgão da APF que não possui uma Política de Segurança da Informação, ficando assim mais vulnerável a incidentes de segurança, apesar de sua missão estratégica para a nação.

1.2. PROBLEMA DE PESQUISA

Diante do exposto, o problema de pesquisa foi apresentado da seguinte forma:

- Quais são os Fatores Críticos de Sucesso para a implantação de uma Política de Segurança da Informação no órgão da APF estudado?

1.3. OBJETIVOS DO ESTUDO

O objetivo foi disponibilizar informações de interesse para aplicar uma Política de Segurança da Informação (PSI) no órgão da APF estudado.



II Simposio Internacional de Gestao de Projetos (II Singep)

Simposio Internacional de Inovacao e Sustentabilidade (I S2IS)

2. REFERENCIAL TEÓRICO

2.1. FATORES CRÍTICOS DE SUCESSO

No final dos anos 70 e início dos 80, as organizações encontraram-se no meio de uma revolução de informações. O crescimento dos sistemas de informação nas organizações resultou na produção de quantidades significativas de informações para análise e tomada de decisão (CARALLI, 2004). Ainda, segundo Caralli (2004), haviam indicativos de que a explosão da informação iria continuar com a chegada do computador pessoal e crescente desenvolvimento dos sistemas de TI.

Rockart inseriu o conceito de FCS na hierarquia dos conceitos de gerenciamento em 1979. Originalmente criados para desenvolver o alinhamento de TI com o planejamento estratégico da organização. Hoje, as palavras “fatores críticos de sucesso” são amplamente conhecidas nas organizações, juntamente com outros termos relativos ao gerenciamento.

Os Fatores Críticos de Sucesso foram definidos por Rockart (1979), como algumas áreas de atividade chave, cujos resultados favoráveis são absolutamente necessários para os gerentes atingirem seus objetivos.

No entanto, de acordo com Caralli (2004), os FCS ajudam as organizações a priorizar suas atividades para desenvolver estratégias de negócio com segurança. Usando os fatores críticos de sucesso como um filtro, os gestores poderiam então identificar a informação mais importante para a tomada de decisões empresariais críticas.

2.1.1. A EVOLUÇÃO DO MÉTODO

O desenvolvimento do método de identificação dos FCS continuou e muitas definições de FCS, ao nível do planejamento estratégico foram apresentadas, mas no trabalho de Bullen e Rockart (1981) é fornecido um útil resumo de definições de FCS:

- áreas-chaves de atividades nas quais os resultados favoráveis são absolutamente necessários para alcance das metas;
- áreas-chaves onde tudo deve funcionar bem para o negócio prosperar;
- fatores que são críticos para o sucesso da organização;
- áreas-chaves de atividades que devem receber constante e cuidadosa atenção da gerência;
- um número relativamente pequeno de assuntos verdadeiramente importantes, nos quais um gerente deve focar sua atenção.

Caralli (2004) afirma que os FCS são geralmente descritos dentro da esfera de influência de um gerente em particular, mas existem muitos níveis de gestão em uma organização, e cada um dos quais pode ter diferentes ambientes operacionais.



II Simposio Internacional de Gestao de Projetos (II Singep) Simposio Internacional de Inovacao e Sustentabilidade (I S2IS)

2.1.2. USO DOS CONCEITOS DE FCS

Discutidos os conceitos de FCS em conjunto com outros conceitos gerenciais, Bullen e Rockart (1981) apontam os três principais usos dos mesmos:

- Ajudar um gerente individual a determinar suas necessidades de informação;
- Ajudar uma organização em seu processo de planejamento geral anual ou de longo prazo;
- Ajudar uma organização em seus sistemas de informação no processo de planejamento.

2.1.3. BUSCANDO AS INFORMAÇÕES QUE OS GESTORES NECESSITAM

Conforme Bullen e Rockart (1981), o uso dos conceitos discutidos é um processo *top-down*. Trata-se de um método empírico, baseado em questionários estruturados, com técnicas que auxiliam os entrevistadores na identificação dos FCS.

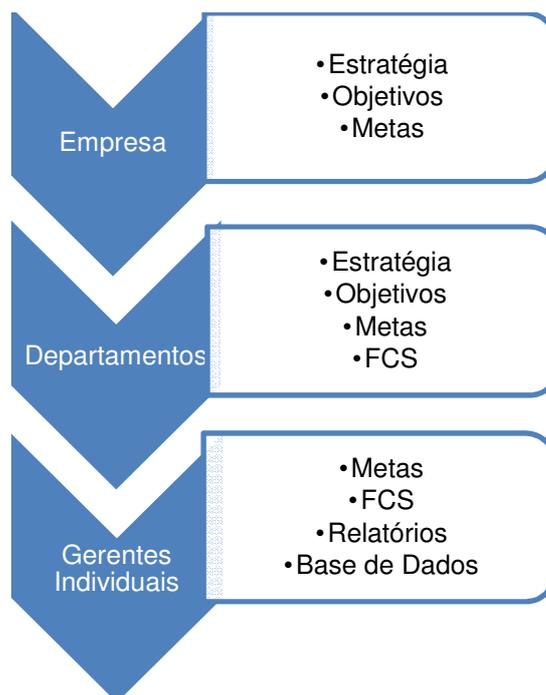


Figura 2 - Processo dos FCS utilizado na determinação das informações
Fonte: Adaptado de Bullen e Rockart (1981)

O gerente começa a pensar em seu ambiente de negócios, tendo a atenção necessária para as estratégias, objetivos e metas de níveis superiores de sua organização.

Rockart (2002) afirma que desde sua introdução, o conceito de FCS tem provado sua utilidade, ajudando as gerências a focar no que é realmente crítico para as organizações.



II Simposio Internacional de Gestao de Projetos (II Singep)

Simposio Internacional de Inovacao e Sustentabilidade (I S2IS)

2.2. O CICLO DE VIDA DO PRODUTO E OS FATORES CRÍTICOS DE SUCESSO

A implantação e desenvolvimento de uma indústria passam por fases que alguns pesquisadores chamam de ciclo de vida do produto (CVP). Segundo Porter (1986), o modelo CVP é o mais antigo conceito para prever a trajetória provável de uma indústria.

2.2.1. ESTÁGIOS DO CICLO DE VIDA DO PRODUTO

Porter (1986) aborda o assunto através do modelo “Prognósticos das Teorias do Ciclo de Vida do Produto”, baseado nos estágios do CVP descritos a seguir:

- **Introdução** - a fase de introdução do produto é o período de tempo entre o nascimento de catálogo de um produto e seu nascimento comercial. Nessa fase, o crescimento das vendas é lento, têm-se altos investimentos e os lucros praticamente não existem;
- **Crescimento** - pode ser definido como o período de tempo entre o nascimento comercial e a receita mensal máxima para o produto. É a fase onde há o aumento da procura do produto, os lucros crescem, mas também chegam novos competidores;
- **Maturidade** – Há diminuição do ritmo de crescimento das vendas e tendência à estagnação ou redução dos lucros, sendo necessário novamente investir pesado em marketing.
- **Declínio** – As vendas e os lucros caem rapidamente.

2.2.2. CVP E FCS

Porter (1986) deduziu vários prognósticos para cada estágio do CVP, os quais podem ser usados como balizadores para o método de Rockart. É possível deduzir previamente um conjunto de FCS a partir dos mesmos, e validá-los empiricamente, conforme comprovado nas pesquisas de Rocha (2005) e Carneiro (2006).

2.3. DEFINIÇÃO DAS HIPÓTESES

A definição das hipóteses deste estudo partiu da identificação dos aspectos de Porter mais relevantes para o mercado em questão com objetivo de identificar e analisar os FCS, no lançamento de uma PSI no órgão da APF em estudo.

Dentre os prognósticos de Porter, foram considerados aplicáveis ao problema de pesquisa os relativos à fase de introdução, pois a pesquisa refere-se ao lançamento de um produto.



II Simposio Internacional de Gestao de Projetos (II Singep)

Simposio Internacional de Inovacao e Sustentabilidade (I S2IS)

O quadro 1 demonstra a relação entre os aspectos de Porter, FCS utilizados, hipóteses formuladas e respectivas questões-chave.

ASPECTOS DE PORTER	FCS	HIPÓTESES	QUESTÕES CHAVE
Compradores e comportamento dos compradores	<p>Apoio da alta direção</p> <p>Adoção rápida de novos hábitos</p> <p>Motivação institucional</p> <p>Definição de papéis e responsabilidades</p>	<p>Hipótese I</p> <p>A inércia de usuários e gerentes (resistindo à adoção de hábitos mais seguros no manuseio da informação) é um FCS no lançamento de uma PSI no IRD.</p>	<p>O apoio da alta direção (com envolvimento prévio) é um FCS no lançamento de uma PSI no IRD?</p> <p>A adoção rápida de novos hábitos é um FCS no lançamento de uma PSI no IRD?</p> <p>A motivação institucional é um FCS no lançamento de uma PSI no IRD?</p> <p>A definição de papéis e responsabilidades é um FCS no lançamento de uma PSI no IRD?</p>
Marketing	Campanha de endomarketing	<p>Hipótese II</p> <p>Uma campanha de endomarketing é um Fator Crítico de Sucesso no lançamento de uma PSI no IRD.</p>	<p>A difusão de manuais/boletins com as características da PSI é um FCS no lançamento de uma PSI no IRD?</p>
Fabricação e Distribuição	Mão de obra especializada	<p>Hipótese III</p> <p>A mão de obra especializada em Segurança da Informação é um Fator Crítico de Sucesso no lançamento de uma PSI no IRD.</p>	<p>Os responsáveis pela PSI do IRD devem ser profissionais especializados em Segurança da Informação?</p> <p>A qualificação prévia de um gerente de Segurança da Informação é um FCS no lançamento de uma PSI no IRD?</p>

Quadro 1 - Relacionamento entre os aspectos de Porter, FCS, hipóteses e questões-chave
Fonte: Elaboração própria



II Simposio Internacional de Gestao de Projetos (II Singep)

Simposio Internacional de Inovacao e Sustentabilidade (I S2IS)

3. METODOLOGIA

3.1. O MÉTODO

O método definido para realização desta pesquisa foi o hipotético-dedutivo de Popper (1975), de Karl Popper (1902-94).

O “Racionalismo Crítico” é uma linha do pensamento filosófico que encoraja um estilo de pensar direcionado para problemas concretos, num sentido prático, buscando soluções efetivas (LIMA, 2008).

O método inicia pela percepção de uma lacuna nos conhecimentos, o problema (P1), para o qual são formuladas hipóteses como solução provisória (TT) e, pelo processo de inferência dedutiva, se testa a predição da ocorrência de fenômenos abrangidos pelas hipóteses visando à eliminação de erros (EE), e novos problemas a partir deste ponto do processo (P2). O esquema a seguir foi sugerido pelo autor para ilustrar o processo:



Figura 3 - Fórmula do processo Hipotético-Dedutivo

Fonte: Popper, 1975

Assim, foram desenvolvidas hipóteses como solução provisória para o problema, as quais foram testadas por meio da coleta de informações em pesquisa de campo e analisados estatisticamente os resultados obtidos.

3.2. UNIVERSO E AMOSTRA

O universo da pesquisa são os servidores públicos, usuários dos serviços de TI, dos níveis estratégico, tático e operacional, totalizando 265 servidores de todas as áreas do órgão. Sendo que destes, apenas 16 (6%) tem menos de 5 anos na empresa, 24 (9%) tem entre 5 e 10 anos na empresa, e 85% tem mais de 10 anos de empresa. Tais números indicam que o universo da pesquisa é, teoricamente, homogêneo quanto ao conhecimento dos processos da instituição.

Decidiu-se então dividir o universo em dois grupos distintos para posterior amostragem, conforme abaixo:

- Gerentes de todos os níveis, os quais são servidores públicos em cargos de confiança. Totalizando 33 servidores;

- Demais usuários, também servidores públicos, mas sem cargos de confiança. Totalizando 232 servidores.



II Simposio Internacional de Gestao de Projetos (II Singep)

Simposio Internacional de Inovacao e Sustentabilidade (I S2IS)

As amostras desta pesquisa são probabilísticas, sendo estratificadas em dois grupos e assim caracterizadas:

- Amostra de usuários com cargos de confiança, respondentes desse estrato que devolveram o questionário. Total de 27 respondentes.
- Amostra de usuários sem cargos de confiança, respondentes desse estrato que devolveram o mesmo questionário. Total de 93 respondentes.

1.1 COLETA DE DADOS

A coleta de dados nesta pesquisa foi realizada por meio da aplicação de um questionário estruturado não disfarçado que buscou dados para ordenar e validar os FCS na implantação de uma Política de Segurança da Informação no órgão da APF em estudo.

A escala escolhida para o instrumento de coleta de dados desta pesquisa foi o de comparação pareada, onde os respondentes foram solicitados a comparar dois FCS de cada vez em um conjunto de vários FCS, o que permitiu a ordenação destes pelo grau de importância conforme percepção dos respondentes. Esta técnica consiste em comparar todos os pares possíveis do conjunto apresentado. Assim, na presente pesquisa, o conjunto apresentado foi constituído pelos 7 FCS, combinados 2 a 2, resultando em 21 combinações possíveis.

1.2 TRATAMENTO DOS DADOS

Os resultados obtidos da pesquisa de campo a partir das questões que apuram a ordem de priorização dos Fatores Críticos de Sucesso foram tabulados e submetidos ao teste de normalidade Kolmogorov-Smirnov que, conforme sugerido por Mattar (1994), por “tirar proveito da natureza ordinal da informação”, é o que mais se adequa à natureza das variáveis ordinais e ao tipo de amostra estudada.

Com esse teste buscou-se validar estatisticamente os FCS estudados.

2 ANÁLISE DOS RESULTADOS

2.1 MÉTODO KOLMOGOROV-SMIRNOV

Conforme Siegel (1975), o teste Kolmogorov-Smirnov indica se “os valores da amostra podem razoavelmente ser considerados como provenientes de uma população com determinada distribuição teórica”. O que é feito determinando-se o ponto em que a distribuição teórica e a observada apontam maior diferença.



II Simposio Internacional de Gestao de Projetos (II Singep)

Simposio Internacional de Inovacao e Sustentabilidade (I S2IS)

De acordo com Mattar (1994), o método Kolmogorov-Smirnov além de “tirar proveito da natureza ordinal da informação”, tem aplicação simplificada, sendo um poderoso instrumento para a identificação de resultados estatísticos significativos.

A prova de uma amostra com esse método é uma prova de aderência. Ou seja, refere-se ao grau de concordância entre a distribuição teórica específica.

2.2 INTERPRETAÇÃO DOS DADOS

Os dados coletados no questionário de campo foram submetidos ao teste de Kolmogorov-Smirnov, onde os Fatores Críticos de Sucesso foram ordenados do mais para o menos crítico, ordem decrescente da pontuação absoluta (pa).

As tabelas 1 e 2 apresentam os resultados obtidos para os funcionários com e sem cargos de confiança, respectivamente.

Tabela 1 - Resultado do método Kolmogorov-Smirnov, funcionários com cargos de confiança.

Fatores Críticos de Sucesso	Pontuação Absoluta (pa)	Pontuação Relativa $Pr=pa/pt$	Pontuação Relativa Acumulada pra	Pontuação Relativa Teórica $prt=1/7$	Pontuação Relativa Acumulada Teórica $prta=prt$	Diferença entre a Pontuação Real e Teórica $\Delta=pra-prta$
Definição de papéis e responsabilidades	113	0,199	0,199	0,143	0,143	0,056
Motivação institucional	101	0,178	0,377	0,143	0,286	0,092
Qualificação prévia de um gerente de Segurança da Informação	78	0,138	0,515	0,143	0,429	0,086
Profissionais especializados em Segurança da Informação	77	0,136	0,651	0,143	0,571	0,079
Apoio da alta direção	76	0,134	0,785	0,143	0,714	0,071
Adoção rápida de novos hábitos de trabalho	71	0,125	0,910	0,143	0,857	0,053
Difusão de manuais/boletins com as características da PSI	51	0,090	1,000	0,143	1,000	0,000
TOTAL DE PONTOS (pt)	567					

Fonte: Elaboração própria

Como é possível observar a partir da tabela acima, a diferença máxima acumulada $D = 0,092$ é menor do que o valor tabelado $D_{27} = 0,26$ para uma amostra de 27 componentes e grau de significância $\alpha=0,05$.

Com isso, pode-se afirmar que dois Fatores Críticos de Sucesso foram validados por todo o grupo da amostra:

1. Definição de papéis e responsabilidades;
2. Motivação institucional.

Estes fatores apresentaram grau de aceitação considerável, o que contribui para validar a consistência dos resultados obtidos.



II Simposio Internacional de Gestao de Projetos (II Singep)

Simposio Internacional de Inovacao e Sustentabilidade (I S2IS)

Tabela 2 - Resultado do método Kolmogorov-Smirnov, funcionários sem cargos de confiança.

Fatores Críticos de Sucesso	Pontuação Absoluta (pa)	Pontuação Relativa $P_r=pa/pt$	Pontuação Relativa Acumulada pra	Pontuação Relativa Teórica $p_{rt}=1/7$	Pontuação Relativa Acumulada Teórica $p_{rta}=p_{rt}$	Diferença entre a Pontuação Real e Teórica $\Delta=p_{ra}-p_{rta}$
Definição de papéis e responsabilidades	341	0,174	0,199	0,143	0,143	0,056
Motivação institucional	337	0,172	0,346	0,143	0,286	0,061
Qualificação prévia de um gerente de Segurança da Informação	332	0,170	0,516	0,143	0,429	0,088
Profissionais especializados em Segurança da Informação	320	0,164	0,680	0,143	0,571	0,108
Apoio da alta direção	220	0,112	0,792	0,143	0,714	0,078
Adoção rápida de novos hábitos de trabalho	214	0,109	0,901	0,143	0,857	0,044
Difusão de manuais/boletins com as características da PSI	193	0,099	1,000	0,143	1,000	0,000
TOTAL DE PONTOS (pt)	1957					

Fonte: Elaboração própria

Como é possível observar a partir da tabela acima, a diferença máxima acumulada $D = 0,108$ é menor do que o valor tabelado $D_{93} = 0,141$ para uma amostra de 93 componentes e grau de significância $\alpha=0,05$.

Com isso, pode-se afirmar que quatro Fatores Críticos de Sucesso foram validados por todo o grupo da amostra:

1. Definição de papéis e responsabilidades;
2. Motivação institucional;
3. Qualificação prévia de um gerente de segurança;
4. Profissionais especializados em segurança da informação.

Estes fatores apresentaram grau de aceitação considerável, o que contribui para validar a consistência dos resultados obtidos.

4.3 TESTAGEM DAS HIPÓTESES

A metodologia utilizada se baseia no teste de falseabilidade das hipóteses. Para tal, foram aplicados testes estatísticos adequados à natureza das variáveis e amostras analisadas, e assim verificou-se o grau de significância dos resultados obtidos.

Sendo assim, cada FCS deduzido dos prognósticos de Porter para a fase de lançamento do CVP foi avaliado segundo a visão dos respondentes através de um questionário estruturado.

Os resultados coletados foram tabulados e tratados estatisticamente, podendo-se assim analisar cada hipótese levantada, validá-la totalmente ou parcialmente, ou ainda refutá-la.



II Simposio Internacional de Gestao de Projetos (II Singep)

Simposio Internacional de Inovacao e Sustentabilidade (I S2IS)

4.3.1. HIPÓTESE 1

-A inércia de usuários e gerentes (resistindo à adoção de hábitos mais seguros no manuseio da informação) é um FCS no lançamento de uma PSI no IRD.

Esta hipótese foi validada parcialmente por ambas as amostras, chefes e usuários, pois apenas 2 dos 4 FCS foram validados: Definição de papéis e responsabilidades; e motivação institucional.

4.3.2. HIPÓTESE 2

-Uma campanha de endomarketing é um Fator Crítico de Sucesso no lançamento de uma PSI no IRD.

Esta hipótese foi refutada por ambas as amostras, chefes e usuários.

4.3.3. HIPÓTESE 3

-A mão de obra especializada em Segurança da Informação é um Fator Crítico de Sucesso no lançamento de uma PSI no IRD.

Esta hipótese foi refutada pela amostra chefes e validada totalmente pela amostra usuários.



II Simpósio Internacional de Gestão de Projetos (II Singep) Simpósio Internacional de Inovação e Sustentabilidade (I S2IS)

5. CONCLUSÃO

Após análise estatística das amostras, concluiu-se que somente 2 dos 7 FCS para a implantação de uma Política de Segurança da Informação no órgão da APF estudado, deduzidos dos prognósticos de Porter para as diferentes fases do ciclo de vida de um produto, foram validados pela amostra de gerentes, enquanto na amostra de usuários foram validados 4 FCS, conforme quadro a seguir:

FCS Validados	Amostra
Definição de papéis e responsabilidades Motivação institucional	Gerentes - Usuários com cargos de confiança
Definição de papéis e responsabilidades Motivação institucional Qualificação prévia de um gerente de segurança da informação Profissionais especializados em segurança da informação	Usuários - Usuários sem cargos de confiança

Quadro 1 - FCS validados x Amostra
Fonte: Elaboração própria

Pode-se afirmar que os resultados quando contextualizados em relação ao problema formulado apontaram os dois FCS mais importantes, validados pelas duas amostras, para o lançamento de uma PSI no órgão da APF estudado: definição de papéis e responsabilidades e motivação institucional.

Ou seja, é possível inferir que esses itens devem ser focados para que uma PSI seja lançada com sucesso no mesmo e tenha sua sustentabilidade assegurada.

A pesquisa apontou também não existir consenso entre as amostras quanto aos dois outros FCS validados somente pela amostra de usuários sem cargos de confiança: qualificação prévia de um gerente de segurança da informação e profissionais especializados em segurança da informação.

Não foi objeto de o presente artigo determinar a causa de possíveis divergências entre as amostras, mas o resultado sugere que esses itens também merecem atenção.

A refutação do FCS “difusão de manuais/boletins com as características da PSI” vai de encontro a norma ISO/IEC 27002, a qual ressalta que a PSI deve ser amplamente divulgada na organização. Tal refutação sugere que esta questão não tenha sido corretamente interpretada pelos respondentes, talvez por falta de clareza na elaboração do questionário.

Pode-se afirmar então que o objetivo da presente pesquisa foi alcançado, e que as informações disponibilizadas por este trabalho poderão ser usadas pelo órgão da APF estudado em um projeto interno de Segurança da Informação que depois de montado e implantado transmita aos usuários que seus dados estão guardados em segurança.



II Simpósio Internacional de Gestão de Projetos (II Singep) Simpósio Internacional de Inovação e Sustentabilidade (I S2IS)

6. REFERÊNCIAS

ARAÚJO, Evandro Nicomedes; ROCHA, Elisa Maria Pinto da. Trajetória da sociedade da informação no Brasil: proposta de mensuração por meio de um indicador sintético. **Ciência da Informação**, Brasília, v. 38, n. 3, p.9-20, dez. 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. **NBR ISO/IEC 17799**: tecnologia da informação - código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

BULLEN, Christine; ROCKART, John. **A Primer on Critical Success Factors. Working Paper, Alfred Sloan School of Management.** Center for Information Systems Research, no.69, 1981.

CARALLI, Richard. **The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management.** CMU/SEI-2004-TR-010. Software Engineering Institute, Carnegie Mellon, Jul 2004.

CARNEIRO, Oscar Augusto Cunha. **Fatores Críticos de Sucesso no lançamento (start-up) de pneus remoldados de automóveis, camionetas, camionetes e seus rebocados leves certificados pelos organismos acreditados pelo INMETRO.** 2006. 123 f. Dissertação (Mestrado) - Universidade Federal Fluminense, Niterói, 2006. Cap. 1.

ERNST & YOUNG. **Global information security survey.** Disponível em: <[http://www.ey.com/Publication/vwLUAssets/13%2AA_Pesquisa_GISS/\\$FILE/13](http://www.ey.com/Publication/vwLUAssets/13%2AA_Pesquisa_GISS/$FILE/13)

[%C2%AA_GISS_report.pdf](#) > Acesso em: 2 mar. 2012.

LIMA, Luiz Fernando F. de M.; Quintella, Heitor M. **Percepção de segurança em sistemas de informação e sua relação com a qualidade percebida de serviços, entre as diretorias do Inmetro, IV CONGRESSO NACIONAL DE EXCELÊNCIA EM GESTÃO**, 22 páginas, 2008.

MATTAR, Fauze N. **Pesquisa de Marketing.** São Paulo: Atlas, 1994.

OLIVEIRA, Maria Angélica Figueiredo; NUNES, Raul Ceretta; ELLWANGER, Cristiane. **Uma Metodologia Seis Sigma para Implantação de uma Gestão de Segurança da Informação Centrada na Percepção dos Usuários.** In: SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, 9., 2009, Santa Maria. Anais... . Campinas: Unicamp, 2009. p. 173 - 186.

POPPER, Karl Raimund. **A Lógica da Pesquisa Científica.** São Paulo: Cultrix, 1975.

PORTER, Michael E. **Competição - Estratégias competitivas essenciais.** Rio de Janeiro: Campus, 1999.

QUINTELLA, Heitor Luiz Murat de Meirelles; MELLO, Marcio Luiz Liduino de. **A qualidade percebida em um Sistema de Segurança da Informação. Gepros: Gestão da Produção, Operações e Sistemas**, São Paulo, n. , p.11-24, abr. 2008.



II Simposio Internacional de Gestao de Projetos (II Singep) Simposio Internacional de Inovacao e Sustentabilidade (I S2IS)

ROCHA, Henrique. **Fatores Críticos de Sucesso de Start-up de Veículos e a Qualidade (CMMI) no Desenvolvimento de Produtos no Sul Fluminense.** Dissertação (Mestrado em Sistemas de Gestão). Universidade Federal Fluminense, Niterói, 2005.

ROCKART, F.J. Chief executives define their own data needs. **Harvard Business Review**, 1979.

RODRIGUES, Silviane Cristina de Andrade. **Fatores Críticos de Sucesso para o lançamento de serviços de comunicação móvel de dados nas operadoras de telefonia móvel celular no Brasil.** Dissertação (Mestrado), Universidade Federal Fluminense, Niterói, 2005.

SIEGEL, S. **Estatística não-paramétrica: para as Ciências do comportamento.** São Paulo: McGraw-Hill, 1975.

SNEE, Ronald; **3.4 Per Million: Use DMAIC to Make Improvement Part of 'The Way We Work'.** Quality Progress. Set.2007 Disponível em: <<http://www.asq.org/qic/display-item/index.html?item=21249>>. Acesso em 09 Maio de 2012.

TCU - **Acórdão 2308/2010. Avaliação da Governança de Tecnologia da Informação na Administração Pública Federal** Disponível em:<http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20100913/AC_2308_33_10_P.doc>. Acesso em: 20 abril de 2012

TROMPOWSKY, Fundação. **Curso de Fundamentos em Gestão da Segurança da Informação e Comunicações - CFGSIC.** Brasília: Gsic, 2010.