

Proposta de uma política de segurança da informação para um departamento de polícia técnica

Proposal for an information security policy for a department of technical police

Mariana Oliveira Santos¹, Saulo Correa Peixoto¹, Alex Ferreira dos Santos² e Robson Hebraico Cipriano Maniçoba¹

¹Departamento de Ciências e Tecnologias (DCT), Universidade Estadual do Sudoeste da Bahia (UESB), Rua José Moreira Sobrinho s/n, 45206-190, Jequié, BA, Brasil.

²Centro de Ciência e Tecnologia em Energia e Sustentabilidade (CETENS), Universidade Federal do Recôncavo da Bahia (UFRB), Av. Centenário, 697, Bairro Sim, Feira de Santana, BA, Brasil.

Resumo

Este trabalho tem como objetivo comprovar a necessidade e a importância da aplicação de normas de segurança da informação em uma instituição pública e criar uma Política de Segurança da Informação voltada para a mesma. A metodologia teve caráter bibliográfico, de campo e participante. O cenário escolhido para a aplicação foi o Departamento de Polícia Técnica (DPT), mais especificamente a Coordenadoria Regional de Polícia Técnica (CRPT) de Jequié-BA. O viés triangular da pesquisa foi crucial para se chegar a uma análise de conformidade dos principais aspectos relacionados à segurança da informação dentro do órgão público em cotejo com a norma ABNT NBR ISO/IEC 27002. Esses resultados confirmaram que o DPT/CRPT de Jequié-BA necessita urgentemente de um bom gerenciamento de segurança da informação. Também foi realizada uma análise dos objetivos, principais aspectos e padrões da norma ABNT NBR ISO/IEC 27002, procurando obter maior embasamento para em seguida criar a Política de Segurança da Informação, legitimando a necessidade e a importância do estabelecimento e gestão de normas de segurança da informação em uma instituição de segurança pública.

Palavras-chave: Informação, Segurança da Informação, ABNT NBR ISO/IEC 27002

Abstract

This work aimed to demonstrate the necessity and importance of applying standards of information security in a public institution and create an Information Security Policy toward the same. The methodology was bibliographical, of field and participant. The scenario chosen for the application was the Department of Technical Police (DTP), specifically the Regional Coordination of Technical Police (RCTP) of Jequié-BA. The triangular bias of the research was crucial to arrive at an analysis of conformity of the main aspects of information security within the public body in comparison with the standard ISO / IEC 27002. These results confirmed that the DTP/RCTP of Jequié-BA urgently needs a good management of information security. An analysis of the objectives, main aspects and standards of ABNT NBR ISO / IEC 27002 was also performed, seeking better basis to then create the Information Security Policy, legitimizing the need and importance of establishing and managing security standards information in an institution of public safety.

Keywords: Information, Information Security, ABNT NBR ISO/IEC 27002:2005.

Introdução

De acordo com a ABNT NBR ISO/IEC 27002 0, a informação é um ativo essencial para uma organização e consequentemente necessita ser adequadamente protegida. Ainda segundo esta norma, como um resultado do incrível aumento da interconectividade nos ambientes dos negócios, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades. Conforme Netto [1], Segurança da Informação é o processo de proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade.

Existem algumas normas que tratam sobre gestão de Segurança da Informação. A ABNT NBR ISO/IEC 27002 de 2005 possui um conjunto de controles de segurança para a implantação de sistemas de gestão de segurança, contendo também guias para criação de planos de continuidade de negócio, administração de sistemas e de redes, e criação de Políticas de Segurança da Informação. Dividida em 11 seções, essa norma pode ser utilizada para o desenvolvimento de uma boa gestão de Segurança da Informação. Obviamente, nem todos os controles e recomendações são aplicáveis a todos os tipos organizações e pode haver casos cujos controles adicionais venham a ser necessários. Entretanto, essa norma é considerada a mais apropriada para auxiliar na criação de Políticas de Segurança da Informação (PSI).

A Política de Segurança define o conjunto de normas, métodos e procedimento utilizados para a manutenção da Segurança da Informação, devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação [2]. A PSI é uma estrutura de prevenção e proteção dos dados e processos importantes de uma organização, que determina um padrão de segurança para ser seguido por todos os funcionários da organização, incluindo internos e externos, gerentes, corpo técnico e usuários. Deve ser moldada para a organização, obedecendo aos limites da mesma, porém definindo os controles que devem ser seguidos para assegurar uma boa gestão da segurança da informação.

O Departamento de Polícia Técnica da Bahia (DPT/BA) é um órgão de segurança pública que é responsável por planejar, coordenar, dirigir, controlar, fiscalizar e executar os serviços no campo da polícia técnico-científica, realizando perícias, exames, pesquisas e estudos, visando à prova pericial [3]. Um dos motivos para o desenvolvimento dessa pesquisa é a aplicação prática das metodologias consagradas de salvaguarda da informação, tanto no âmbito acadêmico-científico, quanto nas rotinas das organizações em pleno funcionamento.

O objetivo desse trabalho consiste em analisar os aspectos relacionados à segurança da informação do DPT/Coordenadoria Regional de Polícia Técnica (CRPT) de Jequié – BA, comparando com a norma ABNT NBR ISO/IEC 27002:2005, para que seja possível comprovar a necessidade e importância do estabelecimento de normas de segurança da informação em uma instituição de segurança pública e desenvolver uma proposta de Política de Segurança da Informação voltada para tal instituição.

Materiais e Métodos

Tipo de Pesquisa

Vergara [4] apresenta duas taxionomias de tipos de pesquisa consideradas mais importantes. Segundo tal abordagem, a pesquisa pode ser classificada quanto aos fins e quanto aos meios. Quanto aos fins, a pesquisa terá caráter exploratório, explicativo e aplicado, uma vez que objetiva a maior familiaridade com o problema e envolve levantamento bibliográfico, entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado e análise de exemplos, bem como visa identificar os fatores que determinam ou contribuem para a ocorrência dos fenômenos [5]. Quanto aos meios, é uma pesquisa de caráter bibliográfico, de campo e participante.

Universo, amostra e Seleção dos Sujeitos

Constitui o universo da pesquisa o DPT/CRPT de Jequié-BA – que compreende também o Instituto Médico Legal (IML) de Jequié-BA – e o Setor de Tecnologia da Informação na Coordenadoria de Planejamento, Desenvolvimento e Pesquisa em Salvador – BA. Aqui serão realizadas as pesquisas de campo e participante. A população amostral segue a definição de Vergara [6], como sendo não probabilística selecionada por tipicidade. A amostra é composta por uma seleção de cinco peritos em atividade, lotados na Coordenação Regional do DPT e IML, ambos da cidade de Jequié-BA. A Tabela 1 ilustra a caracterização dos entrevistados.

Tabela 1 - Caracterização dos Entrevistados

Código	Titulação	Idade	Cargo	Formação Acadêmica	Tempo no Cargo
E01	Mestre	35	Perito Criminal	Ciências da Computação	07 anos
E02	Mestre	39	Perito Criminal	Química	07 anos
E03	Especialista	35	Perito Criminal	Farmácia	07 anos
E04	Mestre	35	Perito Odonto-legal	Odontologia	07 anos
E05	Especialista	45	Perito Criminal	Administração	07 anos

Coleta de Dados

A coleta de dados foi obtida através das pesquisas bibliográfica, de campo e participante. A pesquisa bibliográfica, fundamentada em livros, revistas especializadas, teses e dissertações, artigos científicos, sites e outras fontes secundárias cujas essências abordavam o tema do objeto de estudo, foi realizada em bibliotecas e bases de dados virtuais no período entre Agosto e Setembro de 2013, a partir da utilização de palavras-chave como: informação, Segurança da Informação, PSI e Norma ISO/IEC 27002.

A pesquisa de campo utilizou o método de entrevista semiestructural (chamadas também de semiabertas) para coleta de dados. Pôde-se criar um roteiro com base nos achados das pesquisas anteriores, que direcionou a entrevista de forma semiaberta. Após a aprovação do Projeto de Pesquisa nº 13305113.9.0000.0055, pelo Comitê de Ética em Pesquisa da Universidade Estadual do Sudoeste da Bahia, foi entrevistado um grupo de cinco peritos ativos, um deles sendo também coordenador da DPT/CRPT de Jequié-BA. Uma *checklist* foi utilizado como método para a pesquisa participante. O objetivo é apontar quais requisitos da norma ISO/IEC 27002 são atendidos pelo órgão. A *checklist* foi desenvolvida por Oliveira [7] e é dividida em Aspectos Organizacionais, Segurança física, Segurança Lógica e Planos de Contingência.

Resultados e Discussão

A entrevista de forma semiestructural foi realizada com o objetivo de entender, através dos profissionais atuantes – que são os usuários das informações geradas e armazenadas no DPT/Jequié-BA – como são os procedimentos, formas de aquisição, armazenamento, trato e descarte de informações, bem como o conhecimento que os mesmos possuem do tema Segurança da Informação.

A *checklist* foi efetuada como um método de análise de conformidade com os padrões de boas práticas de Segurança da Informação propostos pela norma ABNT NBR ISO/IEC 27002: 2005. Com o resultado obtido desta comparação entre o proposto pela norma ISO/IEC 27002 e a forma como é gerida a Segurança da Informação no DPT/Jequié-BA, é possível perceber o quão se faz necessário a concepção e aplicação de uma Política de Segurança da Informação para este órgão e segurança pública.

As entrevistas semiestructurais sofreram uma análise de conteúdo a luz do método de Bardin [8], cujo objetivo é a manipulação de mensagens (conteúdo e expressão desse conteúdo) para evidenciar os indicadores que permitam inferir sobre uma ou outra realidade que não a da mensagem.

A partir dessa análise qualitativa das entrevistas, foi possível gerar um gráfico (Figura 1) que mostra a relação entre as categorias que surgiram com a análise de conteúdo das entrevistas e a opinião dos entrevistados sobre cada categoria.

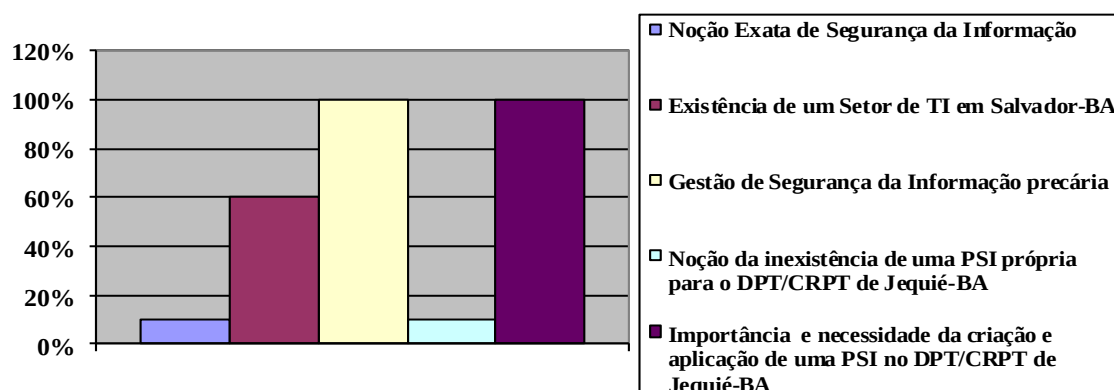


Figura 1 - Categorias x Opinião dos Entrevistados

Fonte: Dados da pesquisa

Fazendo a leitura do Gráfico da Figura1, tem-se que:

- ✓ 10% dos entrevistados possuíam noção exata do que é a Segurança da Informação;
- ✓ 60% dos entrevistados sabiam que o setor responsável pela TI fica localizado apenas em Salvador/BA. Os outros 40% não sabiam se existia algum setor de TI, ou sabiam apenas que não existia um setor específico dentro do DPT/CRPT de Jequié-BA;
- ✓ Todos os entrevistados concordam que a gestão de Segurança da Informação no DPT/CRPT de Jequié-BA é precária;
- ✓ Apenas um dos cinco entrevistados sabia que não existe nenhuma Política de Segurança da Informação aplicada no DPT/CRPT de Jequié-BA no momento;
- ✓ Todos os entrevistados consideram necessário e sumamente importante a criação de uma PSI para o DPT/CRPT de Jequié-BA.

Para obter uma análise de conformidade com a norma ISO/IEC 27002, foi utilizado, além das entrevistas semiestruturais, um modelo de checklist proposto por Oliveira [7]. O objetivo é apontar quais requisitos da norma ABNT NBR ISO/IEC 27002 são atendidos pela instituição. Para cada item relacionado à Segurança da Informação, há dois valores, sendo o primeiro a Situação da organização/empresa, entre 0 (zero) e 10 (dez). O segundo valor corresponde ao grau de importância atribuído ao item, que recebe os seguintes valores: 1 (um) quando o item não for importante; 5 (cinco) quando o item tiver média importância; 10 (dez) quando o item tiver alta importância.

Com a *checklist* respondida, foi feito o seguinte cálculo: em cada item multiplicou-se a nota pelo grau de importância atribuído e em seguida, somam-se esses resultados. Depois o resultado da soma de todos os itens foi dividido pela quantidade de itens, apurando-se a média geral. Essa média representa a conformidade atual com a norma ISO 27002.

Depois de realizados todos os cálculos foram possíveis compará-los com os seguintes níveis de conformidade:

- ✓ 0 a 49%: baixo;
- ✓ 50 a 69%: médio;
- ✓ 70 a 100%: alto.

Os resultados obtidos estão contidos na Tabela 2.

Tabela 2 - Nível de Conformidade com a norma ISO/IEC 27002

DIVISÕES	NÍVEL (%)
Aspectos Organizacionais	21,05
Segurança Física	35,22
Segurança Lógica	29,87
Planos de Contingência	0,0

Os níveis expõem que a conformidade com a norma ABNT ISO/IEC 27002:2005 é baixíssima para um local onde a segurança da informação é extremamente necessária, como é o DPT/BA, por se tratar de um órgão de segurança pública.

Destarte, chega-se a conclusão que, da análise de conteúdo a luz do método de Bardin [8] e a análise dos resultados da *checklist*, o primeiro passo para se resolver esse problema é com a criação de uma PSI adequada para o DPT/CRPT de Jequié-BA.

Com o auxílio dos resultados das entrevistas e da verificação de conformidade utilizando a *checklist*, foi possível montar uma PSI que atenda os requisitos de uma boa gestão de Segurança da Informação, voltada exclusivamente para o DPT/CRPT de Jequié-BA. Foi sugerida na PSI a necessidade de criação de um Comitê de Segurança da Informação dentro da instituição, que tem como objetivo gerenciar a segurança da informação como forma de reduzir os riscos, dentro do DPT/CRPT de Jequié-BA.

Conclusão

Por ser um ativo de suma importância para quaisquer organizações ou empresas, tanto públicas como privadas, a informação deve ser abordada como o bem mais precioso das mesmas e deve ser protegida adequadamente contra ameaças que possam comprometer sua integridade, disponibilidade e/ou confidencialidade. Para isso existe a Segurança da Informação, que se define como uma proteção dos ativos de informação existentes numa determinada organização, preservando seu valor.

Esse trabalho foi realizado seguindo esse princípio e levando em consideração a crescente evolução tecnológica, o avanço dos números de crimes cibernéticos e incidentes de segurança, a situação atual da Segurança da Informação na esfera corporativa, bem como a falta de conscientização e conhecimento de usuários que possuem acesso a essas informações, o que pode ser considerado uma grande falha de segurança.

Sabe-se que as organizações públicas deste país, principalmente as que lidam com informações cruciais, são as que mais necessitam de uma abordagem da importância de se gerenciar a segurança da informação. Observa-se isto por Gualberto [9], quando o mesmo diz que as organizações públicas, como fornecedoras de serviços aos cidadãos, devem prezar pela segurança das informações sob seu encargo já que estas se caracterizam como ativos fundamentais para a eficiente prestação desses serviços. O DPT/CRPT de Jequié-BA é um exemplo, e por questões de afinidade, de geografia e de necessidade, foi a instituição escolhida para o universo da pesquisa.

Os primeiros passos para garantir a gestão de segurança da informação foram dados a partir da criação de uma PSI, seguindo os aspectos determinados pela norma ABNT NBR ISO/IEC 27002, um dos principais objetivos específicos deste trabalho. Conclui-se então que a principal contribuição deste trabalho para a sociedade, em específico para o universo da pesquisa (DPT/CRTP de Jequié-BA), foi a criação dessa PSI, uma forma de corroborar a necessidade e importância da criação de políticas e normas de gestão de segurança da informação para uma instituição de segurança pública.

O processo de descentralização praticado pelo DPT-BA apresenta-se ineficiente no atendimento às demandas de perícias de Computação Forense geradas pelas CRPTs do interior do Estado, pois consegue atender apenas uma ínfima fatia da demanda existente e, ainda assim, sob uma estrutura pautada no improviso, dependente de provocação externa para andamento [10].

Por esse motivo, o presente trabalho limitou-se apenas a comprovar a necessidade de implantação das boas práticas de segurança da informação, definidas pela norma ABNT NBR ISO/IEC 27002, por meio da criação de uma PSI. Esta não foi aplicada por questões de demanda de tempo e burocracia. Assim sendo, sua aplicação pode ser dada no futuro como a continuação e ampliação deste trabalho.

Referências

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. ABNT NBR ISO/IEC 27002, 2005.
- [1] A. S. Netto, “Gestão da Segurança da Informação: fatores que influenciam sua adoção em pequenas e médias empresas”. Dissertação de Mestrado. Universidade Municipal de São Caetano do Sul, São Caetano do Sul/SP, 2007.
- [2] F. N. F. Ferreira e M. T. Araújo, “Política de Segurança da Informação Guia Prático Para Elaboração e Implementação”. 2ª edição, Editora Ciência Moderna, 2008.
- [3] DPT – Departamento de Polícia Técnica. Institucional DPT. Disponível em: <http://www.dpt.ba.gov.br/index.php?site=1&modulo=eva_conteudo&co_cod=23>. Acessado em 20/11/2015.
- [4] S. C. Vergara, “Projetos e Relatórios de Pesquisa em Administração”. 3ª Edição, São Paulo/SP, Editora Atlas, 2000.
- [5] F. S. Kauark; F. C. Manhães e C. H. Medeiros, “Metodologia da Pesquisa – Um Guia Prático”. Itabuna/BA, Editora Via Litterarum, 2010.
- [6] S. C. Vergara, “Métodos de Pesquisa em Administração”. 3ª Edição, São Paulo: Atlas, 2009.
- [7] M. S. Oliveira, “Aplicação das normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 em uma média empresa: Uma visão da implementação”. Trabalho de Conclusão de Curso. Universidade Estadual do Sudoeste da Bahia, Jequié/BA, 2013.
- [8] L. Bardin, “Análise de Conteúdo”. 70ª Edição. Editora Almedina Brasil, São Paulo-SP, 2011.
- [9] E. S. Gualberto, “Um estudo de caso sobre a gestão da segurança da informação em uma organização pública”. Trabalho de Conclusão de Curso de Graduação. Universidade de Brasília. Brasília-DF, 2010.
- [10] S. C. Peixoto, “A Eficiência da Descentralização na Computação Forense do Departamento de Polícia Técnica do Estado da Bahia”. Dissertação de Mestrado, Fundação Getúlio Vargas, Rio de Janeiro/ RJ, 2012.