ISO 27001 – UM ESTUDO SOBRE A APLICAÇÃO DA NORMA

Gustavo Amaral[1], Bruna Mazaro[2], Érico Amaral[3]

[1]Instituto Federal Sul-Rio-Grandense - Campus Bagé - RS - Brasil
[2]Faculdade IDEAU - Campus Bagé - RS - Brasil
[3]Universidade Federal do Pampa - Campus Bagé - RS - Brasil

{gustavo.h.amaral, bmazaro}@gmail.com; ericoamaral@unipampa.edu.br

Resumo. *O presente trabalho busca apontar a relevância de um conjunto de ações para a implementação de um sistema de segurança da informação, alinhado a NBR ISO/IEC 27001 e, aplicado a uma empresa da área de TI. Como resultado desta pesquisa pretende-se identificar a viabilidade desta tarefa na melhoria dos processos de segurança da organização.*

1. Introdução

Atualmente é inegável a presença e a necessidade da Tecnologia da Informação nas empresas dos mais diversos ramos. Percebendo isso, as organizações começaram a investir em formas de manipulação, armazenamento e segurança de seus dados. Nesse sentido deve-se entender que a informação é um ativo valioso e deve ser manipulado de forma segura. Com base nisto a execução correta de controles e a elaboração de uma política de segurança da informação viabiliza um retorno positivo aos investimentos aplicados na organização, minimizando prejuízos e maximizando a continuidade dos negócios (FERRARI, 2008).

A adoção de um Sistema de Gestão da Segurança da Informação (SGSI) é considerada uma decisão estratégica para qualquer empresa, pois isto permite maiores níveis de confiabilidade perante o cliente, além da proteção da informação. Nesse mesmo contexto é necessário adotar ações protetivas e montar um plano de segurança que sugira uma abordagem sistemática de gestão, propondo medidas de apoio a favor da confidencialidade, integridade e disponibilidade deste ativo (RIBAS, 2010).

Estando esta pesquisa em um estágio inicial e frente às questões apontadas, o objetivo deste artigo foi identificar o alinhamento de uma empresa da área de TI, em relação aos controles definidos pela NBR ISO/IEC 27001 e, desta forma propor a implementação da norma, de acordo com a realidade da organização.

2. Gestão de Segurança da Informação

Para garantir a segurança da informação é necessário que sejam adotados um conjunto de procedimentos e controles que assegurem a integridade e a composição dos dados em questão. Dessa forma, pode-se determinar segurança da informação como uma área de conhecimento que é dedicada a proteger esses ativos contra acessos não autorizados, modificações indevidas ou a sua indisponibilidade (SÊMOLA, 2003).

A família de normas ISO 27000 é a principal norma que uma organização pode utilizar para obter certificação empresarial em segurança da informação, sendo a única auditável, servindo de apoio para poder entender os fundamentos, princípios e conceitos que lhe permitem uma melhor gestão dos seus ativos de informação. (SANTOS & SILVA, 2012).

3. Metodologia, Implementação e Resultados Parciais

Como procedimento metodológico realizou-se inicialmente um levantamento bibliográfico sobre a ISO 27001, com o objetivo de identificar os principais ativos e processos de negócio da organização. Na segunda etapa definiu-se o nível de risco de cada processo/ativo, por meio de um *checklist* especifico para esta norma. Os resultados alcançados permitiram, na terceira etapa, definir o conjunto de controles passíveis de serem implementados. Por fim, estas ações culminarão em sugestões de ajustes, através dos quais será possível identificar a real possibilidade de uma certificação de segurança ISO.

Como laboratório para os experimentos desta pesquisa elencou-se uma empresa na área de TI, situada na região sul do Brasil, a qual atua no ramo de desenvolvimento de software e manutenção de hardware, tendo em seu quadro 09 colaboradores.

Seguindo as boas práticas, previstas pela ISO, inicialmente realizou-se uma auditoria em todos os processos que envolvem Tecnologia de Informação. Embora não houvesse uma estrutura claramente definida na organização, o mapeamento de processos identificou os principais elementos, organizados em setores, como: Venda, Assistência técnica e Desenvolvimento. Todos estes conectados através de um sistema de gestão, que registra todas as atividades operacionais e financeiras. A aplicação do *checklist* adaptado de Ferrari (2008) permitiu perceber como é tratada a segurança da informação no âmbito da empresa. Como resultado desta tarefa foi possível identificar quais controles de segurança devem ser implementadas, dados que serviram de subsidio para a elaboração da Declaração de aplicabilidade da ISO 27001.

Tabela 01 – Resumo do resultado da aplicação do *checklist da norma*.

Seção	Descrição	Nível
A	Política de Segurança da Informação	1,25
B	Organizando a Segurança da Informação	1,17
C	Gestão de Ativos	1,25
D	Segurança de Pessoas	2,38
E	Segurança física e do ambiente	2,25
F	Gerenciamento das operações e comunicações	1,96
G	Controle de acesso	2,05
H	Aquisição, desenvolvimento e manutenção de sistemas de informação	2,18
I	Gestão da continuidade do negócio	1,58
J	Conformidade com requisitos legais	2,56
K	Gestão de incidentes de segurança da informação	2,00

O *checklist* foi organizado sobre uma escala Likert de 05 pontos, onde 01 representou o menor valor e 05 o maior índice (controle aplicado e documentado). O compendio resultante das observações apontou para a necessidade de implementação de todas as seções da norma visto que não foram alcançados índices satisfatórios em nenhuma das seções, conforme apresentado na Tabela 01.

5. Conclusão

Espera-se, ao final do projeto, contribuir de forma significativa para a implantação de boas práticas na área de segurança da informação, além de melhorias nos processos da Tecnologia da Informação na empresa, alcançando níveis de maturidade cada vez maiores atingindo o objetivo de implementar o SGSI, proporcionando crescimento contínuo, maior produtividade e lucratividade.

Referências

Ferrari, Graziany Broll (2008) “Implementação de um sistema de gestão da segurança da informação em um ambiente corporativo: uma abordagem teórica e prática”.

Ribas, Carlos Eduardo (2010) “Sistema de gestão de segurança da informação em organizações da área da saúde” – São Paulo.

Santos, Diana Luísa Rocha; Silva, Rita Maria Santos (2012) “Segurança da Informação: a Norma ISO/IEC 27000 e ISO/IEC 27001” – Porto, Portugal.

Sêmola, Marcos (2003) “Gestão da Segurança da Informação: uma visão executiva” – Rio de Janeiro.