ISO 27001 – UMA ABORDAGEM PRÁTICA

AMARAL, L.G.H.[(1)], MAZARO, B.D.[(2)], AMARAL, E.M.H.[(3).]

[(1)] Aluno de graduação do curso de Analise e Desenvolvimentos de Sistema - Instituto Federal Sul-Rio-Grandense – IFSUL Campus Bagé, Rio Grande do Sul, Brasil; Gustavo.h.amaral@gmail.com.

[(2)] Aluna de Especialização em Gestão Estratégica de Tecnologia da Informação – Instituto de Desenvolvimento Educacional do Alto Uruguai (IDEAU) Campus Bagé, Rio Grande do Sul, Brasil; bmazaro@gmail.com.

[(3)] Orientador Prof. Dr. Érico Amaral, Engenharia de Computação, Universidade Federal do Pampa (UNIPAMPA), Campus Bagé, ericoamaral@unipampa.edu.br.

Palavras-Chave: ISO/IEC 27001, Informação, Gestão, Segurança.

INTRODUÇÃO

Inicialmente deve-se entender que a informação é um ativo da empresa. Sendo um ativo, a informação possui valor e deve ser mantida em sigilo e proteção. Essas informações podem existir de diferentes maneiras, tais como, impressas, digitais, armazenadas eletronicamente ou em forma de anotações, etc. O importante é que, independente do modo como as informações existem ou se apresentam, elas devem ter a garantia de um nível adequado de segurança, pensado desde a sua manipulação até o seu armazenamento.

A informação é a nova moeda do mercado, pois em um cenário como o atual, a economia globalizada exige competitividade das empresas para manterem-se no mercado. Percebendo isso, empresas de todos os setores têm investido em formas eficientes de armazenamento de dados, que os auxiliem nas tomadas de decisões.

A gestão da segurança da informação a ser adotada é vista como uma decisão estratégica para a organização, pois assim, a mesma atingirá maiores níveis de confiabilidade perante o cliente, maior competitividade em relação aos concorrentes e, principalmente, irá se prevenir contra ataques externos. Para tal decisão é necessário seguir alguns protocolos, regras e normas que mantenham o padrão do nível de segurança a ser assumido. Nesse sentido, normas são compreendidas como um complexo de orientações e princípios que visam um padrão e uma qualidade na execução de uma tarefa.

O objetivo deste trabalho é propor um modelo de implementação de um Sistema de Gestão de Segurança da Informação (SGSI) aplicado à realidade de uma microempresa do setor da Tecnologia da Informação. Nesse contexto, mostrou-se necessário um estudo sobre todos os conceitos proposto na Norma ISO/IEC 27002, a qual define o conjunto de controles (boas práticas) que consiste em definir um propósito para o desenvolvimento de um SGSI.

REFERENCIAL TEÓRICO

Garantir a segurança da informação não é somente adquirir a proteção de um bom e reconhecido antivírus ou a criação de inúmeras senhas de acesso, é preciso muito mais que isso. 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). Seguindo esse pensamento, a execução correta desses controles associado a uma elaboração de políticas de segurança das informações da empresa em questão trará um retorno positivo aos investimentos aplicados em relação à minimização dos prejuízos e maximização na continuidade dos negócios (FERRARI, 2008).

As normas desempenham um papel essencial na elaboração de um plano de segurança. Portanto, surgiram para dar apoio, aplicar critérios, padrões e instrumentos de controle que se aplicam de alguma forma em cada negócio (SÊMOLA 2003). Nesse mesmo contexto, as normas sugerem uma abordagem sistemática de gestão, fazendo com que adote-se melhores práticas de controles, quantifique-se o nível de risco que pode ser aceito e implemente-se medidas protetivas a favor da confidencialidade, integridade e disponibilidade das informações (DEY, 2007 *apud* RIBAS, 2010).

METODOLOGIA

O desenvolvimento dessa pesquisa será realizado em um conjunto de etapas, previamente definidas, de forma que o primeiro passo é realizar um levantamento bibliográfico da ISO 27001. Tendo em mente os conceitos estudados da normativa e seguindo os três grandes pilares da gestão da segurança da informação (confidencialidade, disponibilidade e integridade) será identificado na empresa em questão os seus mais importantes ativos e processos de negócio relacionados a TI, formando assim uma base para

esse experimento. Num terceiro momento, serão avaliados todos os eventos de riscos que podem estar relacionados a eles, aplicando-se um checklist da normativa, através do qual será possível identificar o conjunto de controles a serem implementados. O próximo passo será reconhecer e parametrizar o nível de segurança da organização e, a partir disto, definir e delinear a aplicação de controles da norma, a fim de minimizar os problemas identificados. Por fim, será possível levantar sugestões de ajustes e visualizar a possibilidade de uma certificação ISO.

RESULTADOS PARCIAIS

Com a norma ISO/IEC 27001 será colocado em prática um sistema de gestão de segurança da informação avaliado e certificado de forma independente, isso permite que seja possível proteger todos os dados financeiros e confidenciais de maneira eficiente, assim minimizando o risco e a probabilidade de serem acessados sem permissão ou ilegalmente. Poderá ser demonstrados compromisso e conformidade nas melhores práticas globais, provando para clientes, fornecedores e demais partes interessadas que a sua segurança é muito fundamental para a operação de sua empresa.

Com a realização desse trabalho percebem-se quais os mecanismos que controlam as ameaças com incidência no controle de acesso, a percepção de intrusos, a criptografia, a assinatura e a proteção de dados armazenados e na recuperação dos mesmos contra possíveis imprevisto importunos.

Neste sentido, está sendo realizado junto a empresa um trabalho que foi inicialmente dividido em etapas como podemos ver abaixo:

1. Reconhecer os ativos e os processos da empresa:
    - Vendas;
    - Assistências técnicas;
    - Desenvolvimentos;
2. Realizar a aplicação de questionários;
3. Aplicar o Checklist – Declaração de aplicabilidade;
4. Aplicar o PDCA;
5. Buscar a melhoria da segurança da informação na empresa;
6. Levantar hipóteses de ajustes;
7. Mostrar a possibilidade de uma certificação.

No momento, estão sendo desenvolvidas as declarações de aplicabilidade (terceiro item da lista) baseada nos levantamentos já realizados junto à empresa.

CONCLUSÕES

A norma ISO/IEC 27001 é um modelo padrão de boas práticas para alcançar níveis de maturidade cada vez maiores na área de Segurança da Informação e atingir o objetivo de implementar o SGSI, sendo assim pode ser usada para avaliar a conformidade pelas partes interessadas internas e externas, onde que o investimento no compromisso da direção e em treinamento dos funcionários reduz a probabilidade de ameaças bem sucedidas.

Espera-se, ao final do projeto, contribuir de forma significativa para a segurança e melhoria dos processos da tecnologia da informação na empresa, 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” – Santa Maria.
- Ribas, Carlos Eduardo (2010) “Sistema de gestão de segurança da informação em organizações da área da saúde” – São Paulo.
- Sêmola, Marcos (2003) “Gestão da Segurança da Informação: uma visão executiva” – Rio de Janeiro.