UNIVERSIDADE FEDERAL DO PARANÁ

AMANDA CRISTINA MOSCHEN

Proposta de implantação ABNT ISO/IEC 27001 – Sistemas de gestão de segurança da informação em uma empresa de seguros de vida.

CURITIBA

2014

AMANDA CRISTINA MOSCHEN

Proposta de implantação ABNT ISO/IEC 27001 – Sistemas de gestão de segurança da informação em uma empresa de seguros de vida.

Projeto técnico apresentado à
Universidade Federal do Paraná
Para obtenção do título de
Especialista em Gestão da
Qualidade.
Orientador: Professor Renato España

CURITIBA

2014

Proposta de implantação ABNT ISO/IEC 27001 – Sistemas de gestão de segurança da informação em uma empresa de seguros de vida.

Amanda Cristina Moschen

Renato España

RESUMO

A Informação é um bem de suma importância para todas as áreas da atividade econômica. A credibilidade de mercado está ligada às técnicas e meios de se proteger contra ataques de hackers, fraudes eletrônicas, espionagem, vandalismos e falhas humanas. Desta forma, o presente artigo tem como objetivo demostrar que as empresas que implementam um sistema de gestão de segurança da informação baseado nas normas ISO melhoram a segurança da informação e aumentam a credibilidade junto ao mercado. Para isso demostraremos neste trabalho formas e técnicas de apoio para a implantação da ABNT ISO/IEC 27001:2006.

Palavras chave: Segurança da Informação, ABNT ISO/IEC 27001:2006, Sistemas de Gestão.

1. INTRODUÇÃO

Devido às novas regulamentações que dizem respeito ao cumprimento de normativos à prevenção da lavagem de dinheiro, a responsabilidade de implementar padrões de segurança em TI, encontra-se entre uma das principais preocupações das organizações.

A informação digital está se tornando um dos maiores produtos da era atual e a segurança da informação compreende um conjunto de medidas que visam proteger

e preservar informações e sistemas de informações, assegurando-lhes integridade, disponibilidade, autenticidade e confiabilidade.

A ABNT ISO/IEC 27001 é a única norma internacional auditável e que define os requisitos para um Sistema Gestão de Segurança da Informação, norma esta que foi desenvolvida para avaliação de risco e gestão da segurança da informação. Além de estabelecer requisitos para proteção de ativos, e segurança das informações dos clientes tornando-se um diferencial competitivo, esta norma também fornece métodos para implantação do SGSI, orientando o processo de implantação do projeto de segurança, sem a definição de hardwares e tecnologias específicas.

A ABNT ISO/IEC 27001 baseia-se no modelo PDCA que possibilita acompanhar o SGSI através de algumas medidas adotadas que tenham impactos na cadeia de valor do negócio da empresa.

Sua finalidade é fornecer uma metodologia para implementação da segurança da informação em uma organização.

2. PROBLEMA

Melhorar a qualidade da segurança na informação dentro de uma empresa de seguros de vida através da certificação NBR ISO/IEC 27001:2006.

3. APRESENTAÇÃO

A seguradora a qual mencionamos neste artigo que por motivos confidenciais não será divulgada o nome, tem sede em Londres e encontra-se operando no Brasil desde 1997, sendo a sede no Brasil localizada em Curitiba.

4. OBJETIVOS

4.1 OBJETIVO GERAL

Buscar a certificação da empresa através da norma ABNT ISO/IEC 27001:2006, procurando trazer benefícios, e maior credibilidade a esta organização.

4.2. OBJETIVOS ESPECÍFICOS

- Identificar problemas dentro da empresa com segurança da informação;

- Determinar a importância da certificação ISO para fortalecimento e credibilidade da empresa;

- Usar a certificação como diferencial em relação à concorrência;

5. REVISÃO DE LITERATURA

5.1 SEGURANÇA DA INFORMAÇÃO - CONCEITUAÇÃO

De acordo com DAWEL (2005), o objetivo da segurança da informação é aprender a lidar e conviver com o risco, e não eliminá-lo completamente, o que na maioria das vezes é impossível. É necessário aprender a controlar os riscos.

A informação de acordo com Rezende e Abreu (2000) é dada como uma interpretação lógica ou natural agregada pelo usuário. A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para organização e, consequentemente necessita ser protegido (NBR ISO/IEC 17799, 2003).

“A informação passa a ser um recurso estratégico para a organização. Ela pode gerar as condições necessárias ao alcance dos objetivos, o cumprimento da missão corporativa e subsidiar elementos básicos para melhoria da competividade. (Brito, Antonialli e Santos, 1997, P.78)

Segundo Rezende e Abreu (2000), a informação desempenha papéis importantes tanto na definição quanto na execução de uma estratégia. Ela ajuda na identificação das ameaças e das oportunidades para a empresa e cria o cenário para uma resposta competitiva mais eficaz.

É evidente que os negócios estão cada vez mais dependentes das tecnologias e, estas, precisam proporcionar confidencialidade, integridade e disponibilidade. Na visão de Albuquerque (2002) há três princípios básicos para garantir a segurança da informação:

• Confidencialidade: a informação somente pode ser acessada por pessoas explicitamente autorizadas. É a proteção dos sistemas de informação para impedir que pessoas não autorizadas tenham acesso;

• Disponibilidade: a informação deve estar disponível no momento em que a mesma for necessária;

• Integridade: a informação deve ser recuperada em sua forma original (no momento em que foi armazenada). É a proteção dos dados ou informações contra modificações intencionais ou acidentais não autorizadas.

Antigamente, a atenção sobre a segurança da informação estava focada na tecnologia. Hoje, o desafio é construir uma relação de confiabilidade com clientes e parceiros. Conforme Rezende e Abreu (2000), as empresas estão procurando dar mais atenção ao ser humano, pois é ele que faz com que as engrenagens empresariais funcionem perfeitas e harmonicamente, buscando um relacionamento cooperativo e satisfatório.

Neste contexto, a segurança visa também aumentar a produtividade dos usuários através de um ambiente mais organizado, proporcionando maior controle sobre os recursos de informática e viabilizando o uso de aplicações de missão crítica.

Segundo Caruso (1993) o crescimento da microinformática foi tão rápido que as empresas foram pegas desprevenidas no trato de seus bens de informação. Os passos a serem dados para se corrigir isso são os seguintes:

- A empresa precisa reconhecer que a informação requer proteção;

- A organização precisa desenvolver planos específicos de proteção;

- O produto a ser instalado deve fornecer segurança de maneira ampla e flexível.

5.2 ABNT ISO/IEC 27001:2006

O padrão Britanico (British Standard) 7799 (BS7799) teve origem em um código de pratica do governo do Reino Unido (Department of Trade and Industry – DTI) de 1993, depois publicado como em 1995 pelo British Standards Intituition (BSI) e revisado em 1999. Quando foi publicada, inicialmente como Norma internacional ISO em dezembro de 2000, a BS7799 parte 1 (BS7799-1) se tornou a ISO 17799. Em outubro de 2005, a British Stantards BS 7799 parte 2 (BS7799-2) foi adotada pela ISO e reidentificada, iniciando uma nova série, a 27000 de padrões internacionais para segurança da informação lançada como norma ISO/IEC 27001 em 2005. No Brasil a ABNT fez a tradução para o português e publicou as normas ABNT NBR ISO/IEC 27002:2005 e ABNT ISO/IEC 27001:2006.

A NBR ISO/IEC 27001:2006 especifica:

A abordagem de processo para a gestão de segurança da informação apresentada nesta norma encoraja que os usuários enfatizem a importância de:

a) *entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer politicas e objetivos para a segurança da informação;*

b) *implementação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócios globais da organização;*

c) *monitoração e análise crítica do desempenho e eficácia do SGSI;*

d) *melhoria continua baseada em medição objetivas. (ABNT, 2006, p.v)*

A ABNT ISO/IEC 27001 é uma das normas de segurança da informação mais utilizadas no mundo e, conforme gráfico abaixo, muitas organizações já foram certificadas nos últimos anos:

Fonte: Pesquisa da ISO sobre Certificações em Normas de Sistemas de Gestão

5.3 INTERPRETAÇÃO DA NORMA ABNT ISO/IEC 27001:2006

Os capítulos nº 1, 2 e 3 referem-se objetivo Referência Normativa e Termos e Definições, sendo todos informativos.

O Capítulo 4 trata da implementação, operação, monitoramento e melhoria do SGSI, neste requisito define-se os membros participantes do SGSI, documentos e registros que devemos manter.

No Capítulo 5 apresenta-se a responsabilidade da direção com a responsabilidade do SGSI, tais como provisionar treinamentos e recursos necessários.

O Capítulo 6 refere-se às auditorias internas, nele são definidas as áreas que devem ser auditadas, sua periodicidade e procedimentos aplicáveis.

O Capítulo 7 é referente a analise critica do SGSI, verificam-se as ações efetuadas pelo SGSI, como se fosse um elemento de controle do mesmo.

Por fim o Requisito 8 que trata da melhoria do SGSI.

5.4 SISTEMA DE GESTÃO SEGURANÇA DA INFORMAÇÃO (SGSI)

De acordo com a ABNT ISO/IEC 27001:2006 a norma tem como objetivo de especificar requisitos para o estabelecimento, implementação, operação, monitoração, analise crítica, manutenção e melhoria do sistema de Gestão de Segurança da Informação (SGSI). A norma está dividida em onze seções específicas, que são: política de segurança da informação; organização da segurança da informação; gestão de ativos; segurança em recursos humanos; segurança física e do ambiente; gestão das operações e comunicações; controle de acesso; aquisição, desenvolvimento e manutenção de sistema de informação; gestão de incidentes de segurança de informação; gestão de continuidade do negócio, e conformidade. São trinta e nove categorias principais de segurança e cada categoria contém um objetivo de controle que podem ser aplicados, assim como algumas diretrizes e informações adicionais para sua implementação. Os requisitos são genéricos de maneira a permitir que seja aplicável a qualquer organização, independente do tipo, tamanho ou natureza. Não é permitida à organização a exclusão de quaisquer requisitos descritos nas seções 4 a 8. Desde que;

“Qualquer exclusão de controles considerada necessária para satisfazer aos critérios de aceitação de riscos precisa ser justificada e as evidências de que os riscos associados foram aceitos pelas pessoas responsáveis precisam ser fornecidas. Onde quaisquer controles forem excluídos, reivindicações de conformidade a esta Norma não são aceitáveis, a menos que tais exclusões não afetem a capacidade da organização e/ou responsabilidade de prover segurança da informação que atenda

os requisitos de segurança determinados pela análise/avaliação de riscos e por requisitos legais e regulamentares aplicáveis (ABNT, 2006, p. 2).”

Fonte: Pesquisa da ISO sobre Certificações em Normas de Sistemas de Gestão

Figura 1 – Ciclo PDCA aplicado aos processos de um Sistema de Gestão de Segurança da Informação. Fonte: ABNT, 2006, p. v.

Se a administração deseja parar para verificar se os níveis de qualidade não atendem os requisitos, o resto da organização compreenderá que o compromisso com a qualidade é verdadeiro. (BERK, 1997).

Ainda nos aconselha Berk, (1997) a avaliação cuidadosa de qualquer melhoria de processo antes da implementação e, os próximos quatro passos do processo de melhoria continua, servem para mitigar o risco associado com a modificação do processo. Os quatros passos são:

- Desenvolvimento de teste;

- Aperfeiçoamento do processo;

- Monitoração das melhorias;

- Continuar a monitorar depois do aperfeiçoamento.

Segundo Campos (1999) “A padronização deve ser vista dentro das empresas, desta mesma forma, como algo que trará melhorias em qualidade, custo, cumprimento de prazo, segurança, etc.”.

Somente após a implantação do SGSI é possível iniciar o processo de certificação deste sistema. A certificação é dada a partir da coleta de evidências (documentos e práticas) do conjunto de controles implantados, e a constatação de que tais controles estão sendo aplicados de maneira eficaz. O SGSI deve passar pela avaliação de um OAC – Organismo de Avaliação da Conformidade que certifica que os processo e atividades estão sendo executados de forma eficiente e consistente com os requisitos da norma ABNT NBR ISO/IEC 27001:2006.

5.5 CICLO PDCA

A norma adota o modelo “Plan-Do-Check-Act” (PDCA). O clico PDCA é um dos métodos mais utilizados para a melhoria de processos. Este método foi desenvolvido na década de 30 pelo americano Shewhat, mas foi Deming que o mais divulgou na década de 50. O ciclo PDCA tem o objetivo de exercer o controle nos processos, podendo ser usado de forma continua em uma organização, são adotados por inúmeras empresas gerando consideráveis efeitos positivos no planejamento da qualidade.

Segundo LIMA (2006) o Ciclo PDCA é uma ferramenta utilizada para a aplicação das ações de controle dos processos, tal como estabelecimento da “diretriz de controle”, planejamento da qualidade, manutenção de padrões e alteração da diretriz de controle, ou seja, realizar melhorias.

Como pode ser observado em sua própria nomenclatura, o ciclo PDCA está divido em quatro fases conforme abaixo;

1 - Plan (P) – Planejamento - Nesta fase se fixa a diretriz de controle, ou seja, definem-se os itens de controle e se estabelecem metas para estes itens. Nesta etapa são decididos os métodos para atingir as metas pré-estabelecidas, que podem ser procedimentos padrões, planos de controle, em suma, uma ação ou uma sequência de ações que levem ao cumprimento da meta. No entanto, quanto maior for o número de informações utilizadas, maior será a necessidade do emprego de

ferramentas apropriadas para coletar, processar e dispor estas informações (WERKEMA,1995).

2 - Do (D) – Execução - Fase em que se executa o plano traçado na fase anterior, exatamente como previsto, de acordo com os procedimentos- ou padrão. Deve-se educar e treinar todas as pessoas envolvidas, antes do início da execução, para que haja comprometimento e a execução seja realizada conforme o planejado. Neste passo, ocorre a coleta de dados, para futura verificação (fase de checagem) (WERKEMA,1995).

3 - Check (C) – Verificação – Fase em que se verificam os resultados da tarefa executada e os comparam com a meta planejada a partir dos dados coletados na fase anterior. É de suma importância o suporte de uma metodologia estatística para que se minimize a possibilidade de erros e haja economia de tempo e recursos. A análise dos dados desta fase indicará se o processo está de acordo com o planejado (WERKEMA,1995).

4 - Act (A) – Atuar corretivamente – Com base nas análises realizadas na etapa anterior (verificação), decide-se no sentido de adotar como padrão o plano proposto, no caso das metas terem sido alcançadas; ou atuar corretivamente sobre as causas que não permitiram que a meta fosse atingida. Ao final dessa fase, origina-se a primeira fase do próximo PDCA (gira o ciclo, voltando ao planejamento), permitindo que se faça o processo de melhoria contínua. De acordo com LIMA apud. RIBEIRO (2006), a conexão entre a última e a primeira fase (Agir - Planejar) é denominada circularidade do Ciclo PDCA.

Figura 2 – Ciclo PDCA (**P**lanejar, **D**esenvolver ou executar, **C**hecar, **A**gir)

De acordo com Campos (2004) o PDCA de melhoria é utilizado para a solução de problemas e atingimentos de metas de forma contínua. Este método é composto por oito etapas: identificação do problema, observação do problema, análise do processo, plano de ação, ação, verificação, padronização e conclusão. De acordo com o mesmo autor, a fase **P** consiste nas etapas de identificação do problema, observação, análise do processo e plano de ação. A fase **D** é da ação ou atuação de acordo com a ação ou plano para bloquear as causas fundamentais. Na fase **C**, é feita a verificação, a confirmação da efetividade do plano de ação para ver se o bloqueio foi efetivo. Na fase **A** são duas etapas: a padronização e a conclusão. Na etapa da padronização em caso de bloqueio efetivo ocorre a eleminação da causa. Na etapa de conclusão ocorre a revisão das atividades e planejamento para os processos futuros.

6. Apresentação de dados

Verificamos que a organização já possui uma preocupação com a segurança da informação, possui vários mecanismos de segurança e politicas de normas internas, podemos citar como exemplo: e-mails criptografados, segurança de senhas de computadores, treinamentos propostos aos colaboradores com a prevenção da segurança da informação, cuidados com armazenamento e descarte de dados, entre outros.

A ISO servirá para apoio e certificação auxiliando a empresa através de seus requisitos sobre segurança da informação. Mostrando ao mercado que a empresa se preocupa e investe em segurança, dando mais confiabilidade de mercado.

Em primeiro momento o projeto de implantação buscará certificar apenas a área de IT, procuramos com isso reduzir o risco do projeto, após a certificação o objetivo é certificar a empresa toda.

7. Métodos de Pesquisa

Incialmente foram levantados dados dos fundamentos básicos da segurança da informação.

Partimos então para conhecimento do mercado e novas tecnologias a serem implantadas na organização a fim escolher às ferramentas mais indicadas para o projeto de implantação.

A seguir se desenvolve o método para a implantação de sistemas de gestão segurança da informação tomando como base a ABNT ISO/IEC 27001:2006.

No momento estamos aguardando aprovação do orçamento para a implantação da norma.

8. Dificuldades na implantação

Há uma resistência comum na maioria dos usuários a qualquer mudança, o ponto positivo é que a organização já adota padrões para a segurança da informação e lavagem de dinheiro, assim acredita-se que haverá menos dificuldade de adaptação às normas. Sendo que terá menos dificuldade em se adaptar as normas.

A implantação de um sistema de gestão de segurança da Informação é difícil de ser realizada e leva tempo para a sua concretização. Ela exige apoio da direção da organização, dedicação constante e qualificação dos profissionais envolvidos.

O orçamento para o ano de 2015 já foi definido pela organização, com isso o projeto para implantação da norma ABNT ISO/IEC 27001:2006 será definido no segundo semestre de 2015.

9. Conclusão

Observamos que a gestão de segurança da informação é um componente estratégico para a organização.

Com o uso do modelo PDCA proposto pela norma, é possível construir projetos em menor tempo sem deixar de atacar as prioridades nos diversos tipos de risco. Com o crescimento de empresas certificadas podemos observar que os fatos são verdadeiros e a preocupação com a segurança da informação é relevante.

Diante do exposto, chegamos à conclusão que ter um certificado de Qualidade ABNT ISO/IEC 27001:2206 é dizer que a organização possui um sistema de qualidade com foco na segurança da informação e se preocupa com seus clientes, obedecendo aos requisitos de uma norma internacional.

Muitas são as vantagens que a organização pode obter com a certificação, podemos citar: credibilidade com o mercado consumidor, confiabilidade do mercado e clientes, menor risco com vazamento de informações relevantes de clientes e da empresa e, melhores condições para controlar e acompanhar o processo.

REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. ABNT, 2006.**

ALBUQUERQUE, Ricardo e RIBEIRO, Bruno. Segurança no Desenvolvimento de Software – Como desenvolver sistemas seguros e avaliar a segurança de aplicações desenvolvidas com base na ISO 15.408. Editora Campus. Rio de Janeiro, 2002.

BERK, Joseph, Administração da qualidade total: aperfeiçoamento contínuo: teoria e prática /; tradução de Cláudia Azevedo: revisão técnica de Antenor Braga Pereira. Editora Ibrasa. São Paulo, 1997.

BRITO, Mozar José de; ANTONIALLI, Luiz Marcelo; SANTOS, Antonio Carlos dos. Tecnologia da informação e processo produtivo de gestão em uma organização cooperativa: um enfoque estratégico. Curitiba, 1997.

CARUSO, Carlos Alberto Antônio. Segurança em microinformática e em redes locais. Editora LTC. Rio de Janeiro, 1993.

CAMPOS, Vicente Falconi. Qualidade Total. Padronização de empresas. Editora de Desenvolvimento Gerencial. Belo horizonte, 1999.

CAMPOS, V. Falconi. Gerenciamento da rotina do trabalho do dia-a-dia. Editora INDG Tecnologia e Serviços Ltda. Belo Horizonte, 2004.

DAWEL, George - A Segurança da Informação nas Empresas. Editora Ciência Moderna. Rio de Janeiro. 2005.

LIMA, Renata de Almeida - Como a relação entre clientes e fornecedores internos à organização pode contribuir para a garantia da qualidade: o caso de uma empresa automobilística. Ouro Preto: UFOP, 2006.

NBR ISO/IEC 17799. Tecnologia da Informação. Código de Prática para Gestão da Segurança da Informação. Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2003.

REZENDE, Denis Alcides e ABREU, Aline França. Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais. Editora Atlas. São Paulo, 2000.

WERKEMA, M. C. C. As ferramentas da qualidade no gerenciamento de processos. Fundação Christiano Ottoni, UFMG. Belo Horizonte, 1995.