UFRGS

MBA Gestão Empresarial 2012/2013

Segurança da Informação: o caso da empresa CF Vigilância.

Aluno: Evaldo Osório Hackmann

Professora Orientadora: Dra. Ângela Freitag Brodbeck

Agosto de 2013

Resumo

Cada vez mais, a segurança da informação faz parte do dia a dia de executivos e demais colaboradores de uma organização. Criar uma cultura de segurança da informação: conjunto de oreientações, norma e política que resguardam o ativo de valor empresarial é vital para a continuidade dos negócios.

Com esse intuito, o objetivo do trabalho em destaque é criar um plano de segurança da informação para empresas de segurança privada. A pesquisa será exploratória, baseando-se no método do estudo de caso (Yin, 2005) contemporâneo e real.

Verificaram-se como principais resultados dessa pesquisa que não havia uma adequada preocupação com tema e, ainda, havia certo amadorismo permeando a relação negocial entre os clientes e a CF Vigilância. Assim, a implementação do plano, com base nas necessidades da organização (Laureano, 2005; ABNT 27002), colaborou de modo definitivo para que a empresa ocupasse lugar de destaque no segmento da segurança privada – prestando serviços especializados e diferenciados – garantindo sua continuidade com respostas mais ágeis, seguras e precisas aos clientes.

Palavras-chave: informação, ativo, segurança, plano, pesquisa e empresa.

1. Introdução

Segurança de informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso e a informação, possibilitando que o negócio da Organização seja realizado e a sua missão seja alcançada (FONTES, 2010). Este conceito pode ser complementado com o que a Norma BS 27000 (ABNT, 2006) cita: “segurança da Informação é a proteção de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades do negócio”.

Sendo assim, pode-se compreender que a segurança da informação trata das regras e procedimentos que envolvem a proteção de um dos mais valiosos ativos (valor) para as empresas, qual seja a informação. Com base no adequado tratamento daquela, as empresas estarão habilitadas a prosperar, bem como a garantir-se de modo sustentável e contínuo em seu ambiente de negócios.

A segurança da informação é fundamental para a continuidade dos negócios visto que as organizações são criadas com a expectativa de permanecerem muitos anos desenvolvendo suas atividades; toda informação deve ser protegida contra desastres físicos (fogo, calor, inundação etc.) e lógicos (vírus, acesso indevido, erro de programas, alteração incorreta etc.). Assim, cada organização deve estar preparada para enfrentar situações de contingência ou desastre que tornem indisponíveis os recursos que possibilitem a continuidade de seu negócio (FONTES, 2010).

Uma boa política de continuidade de negócio garante à organização a possibilidade de realizar o seu trabalho, transpondo as dificuldades apresentadas por obstáculos (físicos, humanos ou lógicos) que impeçam o adequado e regular desenvolvimento de suas atividades empresariais. Isto vem ao encontro do que diz a Norma BS 27000 (ABNT, 2005), quando cita que a boa gestão da continuidade do negócio tem por objetivo não permitir a interrupção das atividades do negócio e proteger os processos críticos contra

efeitos de falhas ou desastres significativos, e assegurar sua retomada em tempo hábil, se for o caso.

A empresa a ser estudada – CF Vigilância – é uma empresa de segurança privada, de pequeno porte, com atuação na Região Sul do Brasil, e apresenta vulnerabilidades tanto em seus sistemas de informação, bem como em infraestrutura para suportar estes sistemas e todas as operações automatizadas. Diante destes problemas reais da empresa e da importância descrita anteriormente com relação aos processos de segurança de informação e continuidade dos negócios instituídos por normas constantes em Governança de TI, surge a seguinte questão de pesquisa: “quais os procedimentos mais adequados para um sistema de gestão da informação para uma empresa de segurança privada?”. Para tanto, o objetivo desta pesquisa é elaborar um plano de segurança da informação para atender as necessidades e garantir a continuidade dos negócios de uma empresa que atua no mercado de segurança privada.

Este artigo encontra-se estruturado da seguinte forma: uma introdução contendo a importância do tema investigado, a questão e o objetivo da pesquisa; a base conceitual que norteou os procedimentos desta pesquisa sobre informação e as normas de segurança de informação; a metodologia da pesquisa, o desenvolvimento da pesquisa e os resultados obtidos, a conclusão e contribuições.

2. Informação

A informação é muito mais do que uma simples compilação ou agrupamento de dados. Ela é o resultado da transformação desses dados de pouco significado incialmente, em um recurso importante e de valor tanto para nossa vida pessoal quanto para a vida profissional (Fontes, 2010).

Dessa maneira, a informação é um ativo de valor e, por isso, dependendo de seu conteúdo, pode representar grande poder para quem a detém. Ela está inserida no contexto da instituição, integrada com os

processos, pessoas e tecnologias daquela (Rezende e Abreu, 2000; Laureano, 2005) conforme simbolizado no esquema abaixo.

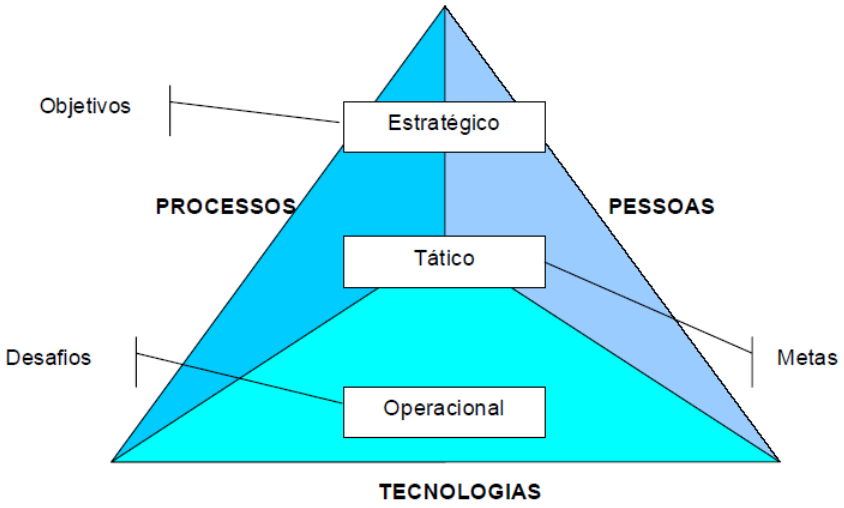

Figura 1: A informação integrada aos processos da Organização.
Fonte: *apud* (Laureano, 2005).

Assim, tendo um valor em si e para quem a possui, a informação deve ser guarnecida, levando-se em conta o tipo de negócio e o porte de cada organização, criando-se uma estrutura justa e eficiente para a sua proteção (Fontes, 2010).

Atualmente, diante da infinita quantidade de informações disponibilizadas nos mais diversos canais de comunicação, o desafio é coletá-la com qualidade para que possa vir a ser utilizada eficientemente pela organização, gerando valor para o seu negócio. Dispor da informação correta, na hora adequada, significa tomar uma decisão de forma ágil e eficiente (Laureano, 2005).

A necessidade de proteger a informação de modo correto, com base nos preceitos da BS 27000 (ABNT, 2005), se revela importantíssima para a sobrevivência das empresas. Com a evolução dos sistemas de comunicação e armazenamento de dados, o uso informação ganhou intensa mobilidade, real inteligência e efetiva capacidade de gestão

(Laureano, 2005). A informação representa a inteligência competitiva dos negócios e é, reconhecidamente, um ativo crítico para a continuidade operacional e saúde da empresa (Sêmola, 2003).

Segundo (Laureano, 2005; Fontes, 2010), podemos classificar as informações do seguinte modo:

a) **Pública** – é aquela que pode ser divulgada ao público em geral sem maiores preocupações ou cuidados para a empresa, e cuja integridade não é vital;
b) **Interna** – se trata da informação que possui restrito público-alvo. Contudo, sua divulgação a alguém não autorizado não causa maiores problemas à empresa. Sua integridade é importante, mas não vital;
c) **Confidencial** – nesta modalidade, a informação deve ficar restrita aos limites da organização. Sua divulgação ou perda pode levar ao desequilíbrio operacional e, eventualmente, prejuízos financeiros ou crises de imagem e credibilidade frente ao público externo, além de permitir vantagem aos concorrentes;
d) **Secreta** – informação extremamente sensível, fator crítico para a continuidade dos negócios da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser limitado a um número reduzido de pessoal. A manipulação desse tipo de informação é vital para a saúde da organização.

A classificação acima é um dos pilares de construção do sistema de segurança de informação da organização. É com apoio na segurança da informação que a organização minimiza os riscos inerentes a sua atividade empresarial, podendo almejar a sua sobrevivência, os resultados positivos e a continuidade de seus negócios de modo indefinido.

Finalmente, o modo correto de trabalhar com a informação é responsável por proporcionar às empresas a possibilidade e a livre escolha de criar e manter vivas as oportunidades negociais em suas respectivas áreas de atuação (Laureano, 2005).

Os princípios básicos da segurança da informação são:

a) **Confidencialidade** – A informação deve ser acessada apenas por pessoas expressamente autorizadas. Assim, se deve impossibilitar que pessoas estranhas à organização ou não autorizadas tenham acesso ao seu conteúdo. O aspecto mais importante, segundo (Albuquerque e Ribeiro, 2002; Laureano, 2005; Fontes, 2010) e garantir a identificação e a autenticidade das partes envolvidas.
b) **Integridade** – Trata-se da garantia de que a informação será acessada em seu conteúdo original primário, ou seja, uma proteção contra adulterações ou modificações acidentais ou intencionais realizadas por entes não autorizados.
c) **Disponibilidade** – A qualquer momento, sempre que necessário a atividade desempenhada, a informação deve estar disponível ao usuário que a busca.

Ao respeitar os princípios básicos supracitados em proporções apropriadas, às Organizações criam uma forma sustentável para o alcance de seus objetivos, pois terão a sua disposição sistemas mais confiáveis (Laureano, 2005).

Há outros princípios que se relacionam com os anteriormente elencados e, de acordo com (Albuquerque e Ribeiro, 2002; Sêmola, 2003; Laureano, 2005; Fontes, 2010), são de desejável observância pelos Sistemas de Segurança da Informação de uma empresa:

a) **Autencidade** – é a comprovação irrefutável (certeza) de origem dos dados ou informações;
b) **Não repúdio** – Impossibilidade de negar o enviou alteração de algum dado ou informação, ou seja, no sentido de eximir-se de culpa ou alegação de que não foi realizada a ação por quem teve acesso ao seu conteúdo;
c) **Legalidade** – Trata-se da aderência de um sistema de informação aos preceitos legais que a regulam;

d) **Privacidade** – A informação pode ser trabalhada, exposta ou alterada, sem que os demais usuários identifiquem o responsável por essas ações;
e) **Auditoria** – Realizasse quando se torna possível a identificação dos rastros de uma informação (origem, alterações, identificação de usuários, data e local).

Citando (Stoneburner, 2001), para o qual um correto Sistemas de Informações surge através da integração entre confidencialidade, integridade, disponibilidade e auditoria, (Laureano, 2005) ilustra a relação destacada:

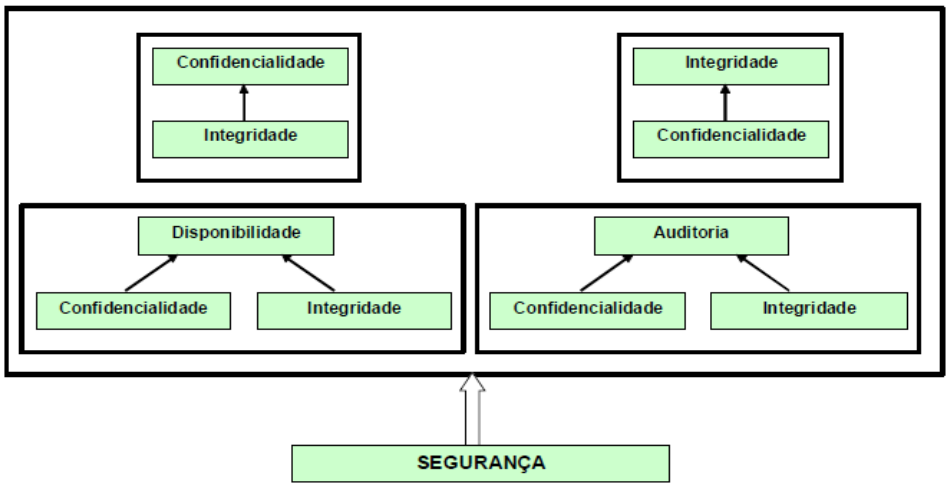

Figura 2: Princípios de uma Sistema de Informação.
Fonte: *apud* (Laureano, 2005).

Realmente, concordamos que a melhor prática de Sistema de Informações surge com a sinergia entre os 04 princípios (confidencialidade, integridade, disponibilidade e auditoria) apresentados no esquema em razão da interdependência entre os mesmos (Stoneburner, 2001).

Dispostos os principais componentes e os parâmetros de um Sistema de Informações (norma técnica e doutrina), apresentaremos alguns modelos nos quais podem se apresentar.

3. Modelos de Segurança de Informação

A escolha de um modelo de Segurança da Informação depende, dentre outros fatores, das necessidades, objetivos, mapeamento dos processos, descrição das atividades, requisitos de segurança, capacidade de investimentos e porte da empresa.

Assim, quanto mais simples for o nível de segurança exigido pela atividade desempenhada pelo ente empresarial, mais simples será a implementação bem como manutenção e melhoria de seu plano de Segurança da Informação.

De acordo com (ABNT 27001, 2006), o sistema de gerenciamento da informação é projetado para assegurar a seleção de controles de segurança adequados para proteger os ativos de informação da Organização.

Os Sistemas de Informação possuem importância fundamental na consecução dos objetivos de negócio da Organização e, consequentemente, para a sua sobrevivência ao longo do tempo. Portanto, tais sistemas de informação devem ser dotados de um nível de segurança que sejam adequados às características e objetivos de negócios de cada Organização.

A seguir, dois modelos de Segurança da Informação – com base em normas técnicas (ABNT 27001, 2006 e ABNT 27002,2005) e doutrina – serão apresentados.

O primeiro traz a relação entre serviços e elementos utilizados para suportar e executar a segurança tecnológica da informação, ao lado de seus relacionamentos preliminares (Stoneburner, 2001).

Nesse caso, os serviços entregues à Organização são divididos em:

a) **Serviços de suporte** – persuasivos e inter-relacionados com inúmeros outros serviços. Ex.: identificação, gerenciamento de chaves de criptografia, administração da segurança, sistemas de proteção;

b) **Serviços de prevenção** – possuem como objetivo impedir que ocorram quebras ou ameaças na segurança do sistema. Ex.: proteção das

comunicações, autenticação de usuário, permissões/autorizações, controles de acesso, não repúdio e transações privadas;

c) **Serviços de detecção e recuperação –** em caso de falha na segurança, deve ser tomada a ação mais precisa e célere de modo que sejam evitados prejuízos à Instituição. Ex.: auditoria, detecção de intrusão e confinamento, verificador de integridade e retorno a normalidade (estado seguro).

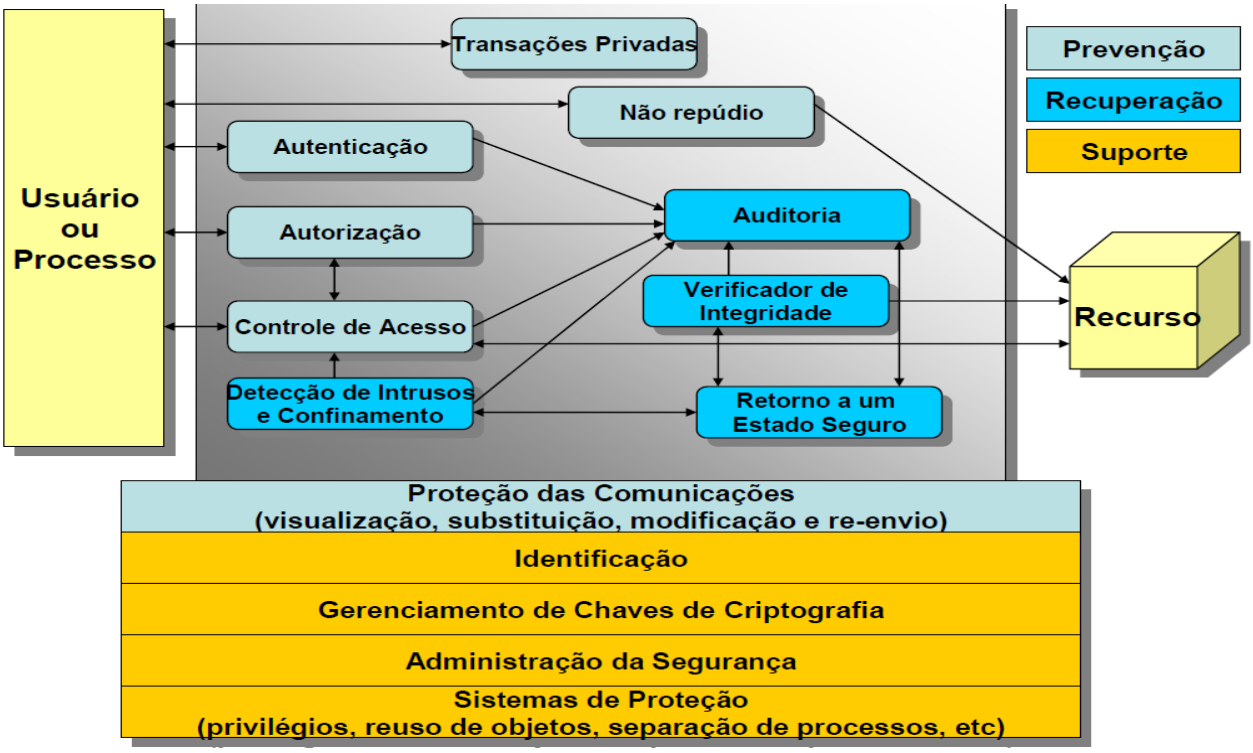

Figura 3: Sistema de Segurança da Informação.
Fonte: Adaptação (Stoneburner, 2001).

O segundo modelo apresentado tem por base o exposto na Norma (ABNT 27001,2006), utilizando-se da metodologia PDCA (*plan, do, check and act*) que embasa e confere suporte aos seus processos.

O esquema a seguir considera as entradas de requisitos de segurança de informação e as expectativas das partes interessadas, e como as ações necessárias e processos de segurança da informação produzidos resultam no atendimento a estes requisitos ou expectativas bem como vinculando o processo às demais seções da Norma (ABNT 27001, 2006).

Figura 4: Ciclo PDCA – Sistema de segurança da Informação.
Fonte: Adaptação (ABNT 27001, 2006).

Assim, forte na Norma (ABNT 27001, 2006 e ABNT 27002, 2005), os *requisitos gerais* para a confecção de um modelo de sistemas de informação adequado devem *estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar o sistema documentado* dentro do contexto das atividades de negócios globais da Organização e os riscos que ela enfrenta.

4. Metodologia de Pesquisa

Esta pesquisa pode ser classificada como exploratória, utilizando o método de estudo de caso uma vez que vai investigar um fenômeno contemporâneo dentro de um contexto real (YIN, 2005). A pesquisa, realizada na empresa Curtinaz & Freitas Vigilância e Segurança Ltda (CF Vigilância), irá propor um plano de segurança de informação que auxilie na continuidade do negócio.

A empresa selecionada - CF Vigilância - é de pequeno porte e desenvolve suas atividades no ramo da segurança privada, possuindo como unidades de negócios: SPP – segurança pessoal privada, escolta armada e a prestação de serviços especializados às Instituições Financeiras. A empresa foi selecionada por conveniência uma vez que o pesquisador é um dos membros da mesma e tem acesso a informações cruciais para esta pesquisa.

As principais etapas desta pesquisa são:

a. Levantamento bibliográfico sobre segurança de informação;

b. Identificação e classificação dos principais itens de segurança de informação expressos na norma BS 27000;

c. Seleção dos entrevistados;

d. Levantamento dos itens de segurança de informação a serem adotados pela empresa em questão;

e. Sugestões e oportunidades de melhorias para continuidade no trabalho;

f. Desenho do plano de implementação de normas de segurança da informação a ser proposta.

A coleta de dados foi realizada através de reuniões específicas individuais e/ou com o grupo de funcionários formado especificamente para trabalhar neste projeto, apresentados no Quadro 1. Além das reuniões, alguns dos participantes foram entrevistados no intuito de confirmar alguns dos processos e elementos de segurança de informação a serem inseridos no plano de implementação (YIN, 2005).

Quadro 1- Grupo de trabalho formado na empresa

COLABORADOR	POSIÇÃO ATUAL	FORMAÇÃO/ESCOLARIDADE	TEMPO DE EMPRESA
Entrevistado 1	Sócio Gerente	Pós Graduado	03 anos
Entrevistado 2	Gerente Operacional	Segundo Grau	03 anos
Entrevistado 3	Supervisor Operacional	Superior	01 ano
Entrevistado 4	Operador de central	Primeiro Grau	01 ano e 06 meses
Entrevistado 5	Coord. Adm. Financeiro	Pós Graduação (incompleto)	01 ano e 10 meses
Entrevistado 6	Escoltista	Primeiro Grau	01 ano e 08 meses
Entrevistado 7	Analista	Segundo Grau	02 anos e 03 meses
Entrevistado 8	Analista	Segundo Grau	02 anos e 02 mês

Os instrumentos de pesquisa utilizados foram: para coleta de dados nas reuniões - os processos e itens de segurança de informação constantes na norma de segurança; para as entrevistas – os itens de segurança de informação identificados nas reuniões.

A análise dos dados coletados utilizou a técnica de análise de conteúdo (YIN, 2005), tendo sido constituída dos seguintes passos: (a) junção de todos os dados obtidos nas anotações de reuniões por item de segurança de informação constante na norma; (b) aplicação da técnica de análise léxica para identificar palavras chaves e verificar expressões similares entre todos os conjuntos de respostas obtidas das anotações das reuniões; (c) relacionamento das expressões e categorias com cada um dos itens de segurança de informação identificado na norma; e, por fim, (d) entrevistas de confirmação das palavras chaves e expressões encontradas cruzadas com os itens da norma.

Os itens mais convergentes serão aqueles selecionados para compor o plano de segurança de informação a ser proposto para a empresa em questão.

5. Desenvolvimento da Pesquisa

Nesta seção serão descritos os seguintes itens: breve contexto da empresa estudada; uma breve descrição de como foram realizados os encontros e as entrevistas; e, os resultados encontrados que compuseram o plano de implementação de segurança de informação para a empresa estudada.

A CF Vigilância, fundada em fevereiro de 2010, tem por objetivo a prestação de serviços especializados em segurança. A empresa atua na área de segurança privada nas seguintes modalidades: SPP (segurança pessoal privada), vigilância e escolta armada.

Igualmente, observando a necessidade do mercado financeiro, especializou-se na prestação de serviços de segurança às Instituições Financeiras: realizando atividades que vão desde a homologação de empresas

prestadoras de serviços, vistorias em agências, elaboração de planos de segurança à atuação preventiva no serviço de pronta-resposta bancária.

Em se tratando da unidade de negócios escolta armada, o cuidado com o manejo das informações é o mesmo. Isto em razão do alto valor agregado das cargas escoltadas (cigarros, pneus, medicamentos, armas, munições, equipamentos eletroeletrônicos, etc...) e a exigência do cumprimento de prazos e precisão nas entregas conforme os compromissos assumidos pelos clientes nas suas respectivas relações comerciais.

Todas essas atividades específicas exigiram da CF Vigilância um maior cuidado no trato dos dados capturados junto aos seus clientes, tendo em vista se tratar de atividades potencialmente visadas por ações delituosas.

Desse modo, no intuito de proteger essas informações (ativos de grande valor), bem como proporcionar que a atividade dos seus parceiros comerciais não sofresse qualquer interrupção ou prejuízo em face de agentes externos ou internos que os prejudicasse (Laureano, 2005), a empresa restou obrigada a investir em segurança da informação.

Foram realizados investimentos em equipamentos (servidores, computadores mais potentes, infraestrutura lógica e física, etc.), softwares (homologação de software, novas licenças, firewall, etc.) e, principalmente, na conscientização e treinamento de seu quadro de colaboradores e sócios. A partir desses investimentos em segurança da informação realizados pela empresa, a CF Vigilância pode alcançar um patamar diferenciado na prestação de serviços em segurança: seja trabalhando para Instituições Financeiras ou empresas que necessitem escoltar suas cargas de forma adequada.

Dado a este contexto, o desenvolvimento de um plano de segurança de informações se tornou premente principalmente com o intuito de garantir que seus serviços prestados continuem a ser desempenhados com qualidade. Além disto, tais normas permitirão que seus colaboradores e sócios absorvam e disseminem as práticas e a cultura de segurança da informação, garantindo a continuidade de seu trabalho e a sua missão no mercado de segurança privada.

5.1. O Desenvolvimento da Pesquisa

Para compor o grupo de pesquisa foram pré-selecionados funcionários de diferentes áreas da empresa estudada os quais, em seu cotidiano laboral, utilizassem sistemas e dados da empresa, sendo eles responsáveis pela disponibilização, manuseio e conhecimento de inúmeras informações. Além destes, foram também convidados a participar os funcionários que das áreas comercial e operacional, ou seja, aqueles que fazem a interface com o cliente, escolta de cargas e aqueles que têm o controle de acesso à base operacional da empresa. Isto permitiu um grupo heterogêneo que possibilitou uma visão mais ampla das necessidades de segurança de informação.

Foram realizadas 04 reuniões [1] com os funcionários selecionados previamente para compor o grupo de trabalho, levando-se em consideração a relevância estratégica de cada qual para a adequada implantação de uma política de segurança. Após cada encontro, aleatoriamente, foram entrevistados dois funcionários para confirmarmos os resultados obtidos em cada oportunidade bem como para verificar suas impressões e para que apontassem as carências da empresa em face do tema.

Na reunião 01, foi realizada uma breve explanação acerca do tema e de sua importância para a CF Vigilância: conceito de informação (ativo de valor), continuidade de negócios, legislação, doutrina e normas técnicas de apoio.

Na reunião 02, discorreu-se sobre medidas físicas de segurança com ênfase à segurança física da base operacional, armazenamento de informações, equipamentos, proteção contra incêndio e monitoramento de atividades por câmeras e sistema de alarme.

Na reunião 03, o assunto proposto foi medidas de TI que cercam o negócio: infraestrutura, telecomunicações, energia, softwares, licenças originais, realização de backup regular, funções de antivírus.

Na reunião 04, tratou-se das providências organizacionais: conscientização de que todos são responsáveis pela segurança do sistema de informação, divisão/segregação de funções, autorizações de acesso (físico e

[1] Para facilitar o ordenamento, denominamos: reunião 01,02, 03 e 04.

virtual), política de contratação de colaboradores, atendimento ao cliente, acesso e confidencialidade de informações.

Reuniões Grupo de Trabalho			
Itens de segurança	**Físicos**	**Tecnologia da Informação**	**Organizacionais (RH)**
X >75%	alarmes	log/senha acesso à rede	recrutamento e seleção
X >50%	câmeras de vídeo	softwares	confidencialidade de informações
50%< X	entrada/saída da sede	cabeamento (dados e energia)	segregação de funções
25%< X	Iluminação	backup de informações	alinhamento às diretrizes da empresa

Tabela 2: Reunião Grupo de Trabalho – Itens de segurança identificados.

Reuniões Grupo de Trabalho X Entrevistas (convergência entre itens)		
Físicos	**Tecnologia da Informação**	**Organizacionais (RH)**
alarmes	log/senha acesso à rede	recrutamento e seleção
câmeras de vídeo	backup de informações	confidencialidade de informações
entrada/saída da sede	cabeamento (dados e energia)	segregação de funções
nihil	Nihil	alinhamento às diretrizes da empresa

Tabela 3: Reunião GT X Entrevistas – Itens de segurança convergentes.

Desse modo, baseando-se nos itens de segurança acima, será realizada a implementação do plano de segurança da informação da CF Vigilância.

5.2. O Plano de Implementação

A elaboração e implementação de um plano de segurança da informação deve seguir uma ordem de importância/prioridades, cotejando-se o que está disposto na Norma (ABNT 27001, 2006; ABNT 27002, 2005) com o que foi definido no planejamento da empresa.

a) **Organizacionais/RH** – os colaboradores e sócios são os principais responsáveis pelo sucesso da implantação de um plano de

segurança da informação (Fontes, 2010; Sêmola, 2003). O respeito às diretrizes da empresa, a conscientização quanto aos aspectos da política de segurança, as rotinas e os procedimentos a serem seguidos são de fundamental importância para elidir as vulnerabilidades que possam afetar a continuidade dos negócios.

a.1) *alinhamento às diretrizes da empresa* – definida a política de segurança de uma empresa, torna-se indispensável que a mesma sirva de balizador para a contratação ou manutenção de seus colaboradores. Pois, caso contrário, a própria organização estaria sabotando o seu plano.

a.2) *recrutamento e seleção* – os responsáveis pelo recrutamento e seleção devem pautar suas escolhas não em preferências pessoais, mas sim no que a organização espera do candidato. Enfim, a seleção tem de ocorrer observando-se as responsabilidades e papeis definidos pelo plano de segurança da informação.

a.3) *confidencialidade das informações* – assegurar que o colaborador tenha ciência da sua responsabilidade no trato das informações. Ressaltar que não serão admitidas falhas nesse processo e que, em caso de comprovação, haverá consequências para quem manejou a informação de modo não desejável.

a.4) *segregação de funções* – deve ser efetivada de modo a garantir o uso correto das informações pela área responsável pela condução do ativo.

b) **Físico/Ambiental** – a segurança da informação requer um cuidado especial com os aspectos de segurança físicos e ambientais: alarme, câmeras de vídeo e controle de acesso são elementos que previnem o ingresso não autorizado de pessoas, dano e interferência nas atividades e instalações da empresa.

b.1) entrada e saída da sede – proteger os locais que contenham o processamento da informação com controles de acesso apropriados e de baixa vulnerabilidade, construir guaritas

e providenciar reforço de alvenaria em áreas sensíveis para a continuidade dos negócios.

b.2) alarmes – criação de sistema de alarmes para identificação de ameaça ou intrusão. Utilização de tecnologia GPRS e analógica ampliar a proteção, reportando à Central de Monitoramento e *smartphones* dos sócios.

b.3) câmeras de vídeo – reforçar a cobertura do perímetro de segurança da empresa com a utilização de câmera de alta qualidade em termos de resolução, utilização de alguns equipamento que permitam a gravação de imagens mesmo em baixa luminosidade e realizar o acesso remoto das imagens.

c) **Tecnologia da Informação** – deve prover para a empresa uma infraestrutura segura, ágil, suficiente e dimensionada ao exercício da atividade empresarial.

6. Contribuições e Conclusões

O trabalho em destaque teve como objetivo fundamental estabelecer um plano de segurança da informação à CF Vigilância – empresa de pequeno porte – que atua no segmento da segurança privada e enfrentava com dificuldades o tema. A implantação do referido plano trouxe à organização uma significativa melhora no trato com a informação bem como um patamar diferenciado na prestação de serviços no mercado em que atua, tendo em vista uma melhor gestão no que tange a esse ativo de valor (informação).

O tratamento adequado da informação, com base num plano moldado às necessidades da empresa (ABNT 27002, 2005), alicerça o crescimento sustentável do ente empresarial e garante a sua continuidade num mercado cada vez mais competitivo.

As medidas tomadas com suporte nessa política de segurança da informação colaboram para que respostas mais céleres, precisas e completas sejam dadas aos clientes. Ao invés do simples trânsito de dados ou informes

imprecisos, o controle e transmissão das informações indicam o correto caminho a ser seguido pelo cliente na busca pelo êxito em suas atividades.

Atualmente, a CF Vigilância tem conseguido ampliar sua carteira de clientes – sobretudo – no segmento escolta armada, no qual se destaca por apresentar um serviço mais abrangente que os concorrentes: atuando em parceria com o setor de inteligência de seus clientes, buscando , tratando e disponibilizando as informações relativas ao transporte de cargas de alto valor agregado, minimizando perdas e otimizando a operação nos modais rodoviário e aéreo.

Com efeito, a pesquisa pode servir de fonte consulta: tanto quanto no que diz respeito ao tema, quanto no que se refere ao método utilizado, a estudantes e profissionais que busquem um maior entendimento acerca da necessidade de implantação de um plano de segurança para empresas de pequeno porte.

A condução da pesquisa encontrou dificuldades para reunir todo o grupo de trabalho numa mesma data em face do andamento do serviço e diferentes escalas de trabalho. Desse modo, sugerimos como melhoria, a quem interessar realizar um trabalho nessa área, que reduza o grupo de trabalho e busque criar um formulário padrão de maneira a diminuir o número de encontros para discussão do tema.

Certamente, não podemos deixar de afirmar o quão fundamental é realizar a implementação de um plano de segurança da informação para a qualquer empresa, independente do porte ou ramo atividade: a seriedade na condução dessa política fará a diferença entre a extinção ou a continuidade de seus negócios.

Referências Bibliográficas

BRODBECK, José Henrique. Gestão da Segurança da Informação. 2005.

FONTES, Eduardo. Segurança da Informação – o usuário faz a diferença. São Paulo: Editora Saraiva, 4ª edição, 2010.

LAUREANO, Marcos Aurélio Pheck. Apostila Gestão de Segurança da Informação. PPGIA/PUCPR. Curitiba, 2005.

Norma NBR ISO/IEC 27002, 2005. Associação Brasileira de Normas Técnica. Rio de Janeiro, 2005.

Norma NBR ISO/IEC 27001, 2006. Associação Brasileira de Normas Técnica. Rio de Janeiro, 2006.

REZENDE, Denis Alcides e ABREU, Aline França. Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais. Editora Atlas. São Paulo, 2004.

SÊMOLA, Marcos. Gestão de Segurança da Informação – Uma Visão Executiva. Editora Campos. Rio de Janeiro, 2003.

STONEBURNER, Gary. Underlying Technical Models for Information Technology Security. NSTI Special Publication, 2001.

YIN, Robert K. Estudo de Caso – Planejamento e Métodos. Porto Alegre: ARTMED, 2005.