RESIGeT On-Line Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica
Uni-FACEF CENTRO UNIVERSITÁRIO DE FRANCA
Vol. 06- Nr. 02 - 2015

Aplicação das normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 em uma média empresa

Mateus Souza Oliveira
Universidade Estadual do Sudoeste da Bahia (UESB)

Saulo Correa Peixoto,
Universidade Estadual do Sudoeste da Bahia (UESB) / Faculdade de Tecnologia e Ciência (FTC)

Alex Ferreira Santos,
Universidade Federal do Recôncavo da Bahia (UFRB)

Robson Hebraico Cipriano Maniçoba,
Universidade Estadual do Sudoeste da Bahia (UESB)

Marcelo Alves Guimarães
Universidade Estadual do Sudoeste da Bahia (UESB)

RESUMO

Este trabalho teve como objetivo a realização de uma análise dos aspectos relacionados à segurança da informação em uma média empresa, antes e depois da implementação das normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002. Adotou metodologia de natureza aplicada, exploratório-descritiva e de abordagem quantitativa e qualitativa. Após realização do estudo, foram percebidas melhorias nos itens relacionados à Segurança da Informação no cenário de estudo. Os resultados obtidos levaram à conclusão de que é possível implementar as normas em empresas de médio porte, com baixo custo, e obter resultados significativamente positivos.

Palavras-chave: Norma ABNT; Segurança da Informação; Implementação de Normas.

ABSTRACT

This work aims to conduct an analysis of aspects related to information security in an average company, before and after in the implementation of the standards ISO / IEC 27001 and ISO / IEC 27002. Adopted the methodology of applied nature, exploratory descriptive and approach quantitative and qualitative . After completion of the study, improvements were noted in items related to Information Security in the study setting. The results led to the conclusion that it is possible to implement the standards in midsize companies, with low cost, and get significantly positive results.

Key-words: Standards ABNT; Information Security; Implementation of Standards.

1. Introdução

Com o avanço da tecnologia e da Internet nos últimos anos, crimes por meio do cyber espaço como fraudes, roubo de senhas e de informações confidenciais, se tornaram notícias frequentes no mundo dos negócios. Grupos de pessoas mal-intencionadas, fazendo uso destes meios, atacam pontos de vulnerabilidade das empresas, gerando caos, danos financeiros e denegrindo a imagem das mesmas no mercado, trazendo enormes prejuízos às instituições.

De acordo com o gráfico na Figura 1, do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), que faz um levantamento anual de incidentes de segurança reportados, o total de notificações em 2011 foi de 399.515, número muito superior ao ano de 2010 (142.844). O número cresce exponencialmente desde 1999, ano em que se iniciou o levantamento, e que contou com apenas 3107 incidentes reportados. 2012 mostrou-se o ano com a maior ocorrência de incidentes, o número de incidentes chegou a 466.029 [CERT.br, 2014].

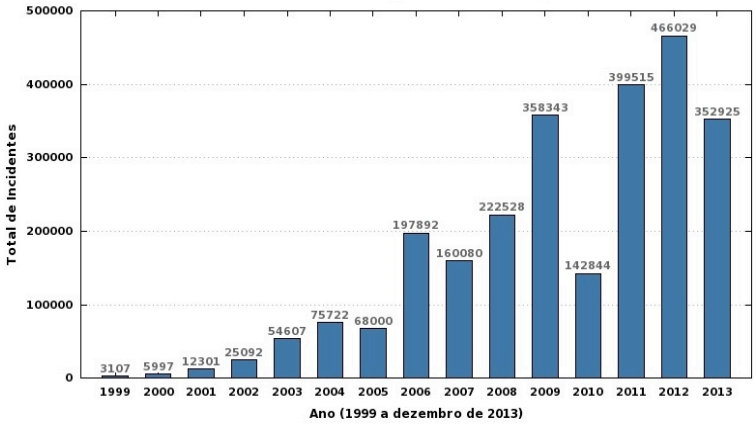

Figura 1. Total de incidentes reportados ao CERT.br por ano. Fonte: [CERT.br, 2014].

Mesmo estando no topo de prioridades das grandes organizações, a Segurança da Informação (SI) é muitas vezes negligenciada nas pequenas e médias empresas (PMEs). Especialistas são unânimes em afirmar que a questão da segurança é mais relevante nas médias empresas, onde o orçamento é reduzido e a estruturação de um setor de segurança, inviável [Ângelo, 2009].

2. Objetivo

O presente estudo teve como objetivo a realização de uma análise dos aspectos relacionados à segurança da informação em uma média empresa, antes e depois da implementação das normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002, demonstrando a importância e eficácia do estabelecimento de normas de SI em organizações de médio porte.

3. Revisão da Literatura

3.1 Segurança da Informação

Em 1986, dois estudantes canadenses, utilizando computadores pessoais e um modem, conseguiram invadir os sistemas da indústria de refrigerantes Pepsi-Cola, realizando entregas de refrigerantes nas casas de amigos e parentes. O fato é considerado por muitos como o "marco zero" dos estudos de segurança em redes de computadores [Moraz, 2006]. A partir de então, a informação, que é o resultado do processamento e da organização de dados, começou a ser mais valorizada pelas organizações.

Nesse âmbito de insegurança do ambiente de tecnologia que cerca principalmente as grandes empresas, surge a Segurança da Informação. A SI é a proteção da informação contra ataques e falhas, ou ainda, "a proteção da informação 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 de negócio" [ABNT NBR ISO/IEC 27002, 2005].

A SI é a responsável pela proteção da informação. Esta deve garantir a continuidade das atividades, a integridade da informação e a disponibilidade da informação e dos serviços da organização. Ramos (2008) aborda sobre a chamada tríade (ou tripé) da SI, como ilustra a Figura 2.

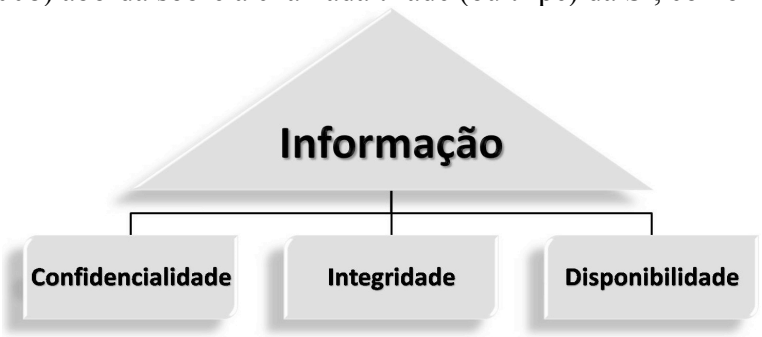

Figura 2. Tríade da Segurança da Informação (aspectos básicos).

A tríade é formada pelos aspectos básicos da SI. São eles:

- Confidencialidade: Trata basicamente do sigilo. É a garantia de que apenas as pessoas autorizadas terão acesso à determinada informação;
- Integridade: Preservar a integridade consiste em proteger a informação contra modificações não autorizadas;
- Disponibilidade: Preza por garantir que a informação esteja disponível a todos que tem autorização, sempre que precisarem. Assim como a integridade, a disponibilidade pode ser comprometida por situações acidentais ou intencionais.

Com a Internet se popularizando e os crimes no ambiente tecnológico aumentando, a preocupação com a Segurança da Informação aumentou, levando os países a criarem normas e padrões, no intuito de organizar a segurança e proteger as organizações.

3.2 Normas de Segurança da Informação

As primeiras normas relacionadas à segurança da informação surgiram na Inglaterra. A preocupação começou com o Departamento de Indústria e Comércio (DTI – *Departament of Trade and Industry's*), que fundou um grupo em 1987 para elaborar um conjunto de critérios de validação, além de uma forma de certificação e um código de boas práticas de segurança da informação. O documento continuou sendo desenvolvido até se tornar um padrão britânico para gestão de SI, nomeado PD 0003. Em 1995, o mesmo se tornou a norma *British Standard* BS7799:1995 [Campos, 2006].

Com a preocupação em saber se as organizações estavam ou não implementando as recomendações da BS7799, foi publicado um novo documento em 1998, a BS7799:1998-2. Esse segundo documento já tinha como objetivo servir como um documento de certificação, pois trazia o conjunto de controles que deveriam ser aplicados para garantir que o código de prática, agora chamado de BS7799:1995-1, estava sendo seguido. Ele foi atualizado para se adequar a outros padrões de sistemas de gestão, e recebeu nova versão em 2002, a BS7799-2:2002 [Campos, 2006].

O código de prática recebeu atualização em 1999, e em 2000 a *International Organization for Standardization* (ISO) homologou a norma, publicada como ISO/IEC 17799:2000. A ISO ainda fez uma atualização da norma, publicando em 2005 a ISO/IEC 17799:2005. Em 2006 foi publicada a BS7799-3:2006, em conformidade com a ISO/IEC 27001, para tratar da avaliação e tratamento de

riscos [BSI Shop, 2006]. Após a criação da família ISO 27000, em 2007, a ISO/IEC 17799 passou a ser chamada de ISO/IEC 27002 [The ISO 27000 Directory].

A norma ISO/IEC 27000 trata de uma explicação da série de normas 27000, ponto de partida para o gerenciamento de segurança, objetivos e vocabulários [ISO/IEC 27000, 2012].

A norma ISO/IEC 27003 trata das diretrizes para a implantação de um Sistema de Gestão da Segurança da Informação. Segundo a própria ISO/IEC 27003, "O propósito desta norma é fornecer diretrizes práticas para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI), na organização, de acordo com a ABNT NBR ISO/IEC 27001:2005" [ABNT NBR ISO/IEC 27003, 2011].

A ISO/IEC 27004 fornece diretrizes para o desenvolvimento de métricas, para realizar avaliação da eficácia de SGSIs e dos controles implementados conforme a ISO/IEC 27001 [ABNT NBR ISO/IEC 27004, 2010].

A ISO/IEC 27005 fornece as diretrizes para o processo de gestão de riscos de SI. Está em conformidade com o modelo de SGSI da ISO/IEC 27001 [ABNT NBR ISO/IEC 27005, 2008].

A ISO/IEC 27006 trata de requisitos para auditorias externas em um SGSI, ou seja, especifica requisitos e fornece orientações para os órgãos que realizam auditoria e certificação de SGSI [ISO, 2011].

A ISO/IEC 15408, também conhecida como "*Common Criteria*" (Critérios comuns), surgiu para unificar padrões de segurança e eliminar as diferenças de critérios. É um padrão internacional de desenvolvimento de produtos seguros, o qual descreve uma lista de critérios (requisitos) de segurança que um produto deve ter. É dividida em três (números de zero a nove devem ser escritos por extenso e acima de 10, em algarismos numéricos, conforme ABNT NBR 6023) partes: ISO/IEC 15408-1 (Introdução e modelo geral), ISO/IEC 15408-2 (Requisitos funcionais de segurança) e ISO/IEC 15408-3 (garantia de requisitos de segurança) [ISO/IEC 15408-1, 1999].

A norma NBR 15999 veio da norma britânica BS 25999-1:2006, e trata sobre Gestão de Continuidade de Negócios (GCN), um importante tópico dentro da SI. É dividido em duas partes: A NBR 15999-1 – Código de Prática, que estabelece os princípios para o entendimento e aprendizado das boas práticas do GCN, e as vantagens para o negócio; e a NBR 15999-2 – Especificações, que aborda os requisitos para a completa implementação de um Sistema de Gestão de Continuidade de Negócios [ABNT NBR 15999-1, 2007; ABNT NBR 15999-2, 2008].

3.3 ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002

A ABNT NBR ISO/IEC 27001 foi desenvolvida a partir da BS 7799-2:2002, sendo uma tradução da ISO/IEC 27001 mantida pela ABNT. Seu objetivo é "prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI)" [ABNT NBR ISO/IEC 27001, 2006].

Doravante, para simplificar, as normas poderão ser mencionadas pelos nomes das suas versões em inglês (ISO/IEC 27001 e ISO/IEC 27002).

A ISO/IEC 27001 descreve um ciclo de atividades que, uma vez seguido, leva à implementação de um SGSI. Adotar um SGSI precisa ser um propósito estratégico da organização, ou seja, sua implementação deve ser adequada aos objetivos, porte, estrutura e necessidades da mesma. Também deve ser levado em consideração o nível de maturidade em segurança, visto que a implementação de um SGSI é um processo que deve evoluir gradativamente [ABNT NBR ISO/IEC 27001, 2006].

A ISO/IEC 27001 utiliza o modelo chamado de PDCA (*Plan-Do-Check-Act*) para estruturar o SGSI. A Figura 3 ilustra o ciclo do PDCA, onde podemos observar as seguintes etapas:

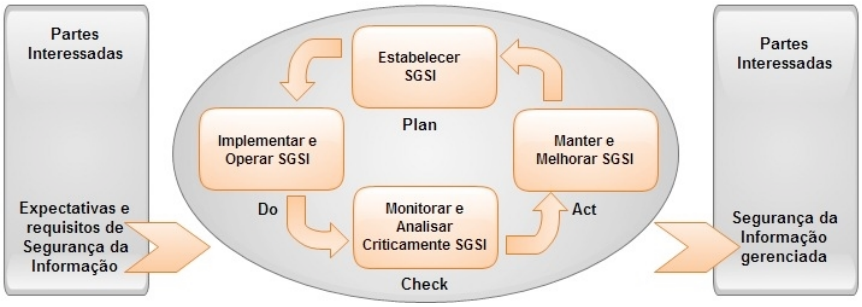

Figura 3. Ciclo PDCA aplicado aos processos de um Sistema de Gestão de Segurança da Informação
Fonte: [Profissionais TI, 2010].

- *Plan* (planejar): Nessa fase é planejado e definido o escopo do SGSI, ou seja, é onde o mesmo será criado de acordo com os objetivos da organização. Nesta fase também serão levantados os riscos e controles de segurança que serão tratados;
- *Do* (fazer): Aqui será implementada a Política de Segurança da Informação (PSI) que sustentará o SGSI, assim como serão criados os controles e procedimentos. Nessa fase é importante a existência de ações de conscientização e treinamentos em segurança da informação;
- *Check* (checar): A análise e monitoramento do SGSI são feitas nessa fase, onde deve ser verificado se a PSI e os controles implementados estão sendo seguidos. Nessa fase poderá ser utilizada uma auditoria, interna ou externa. Por fim, os resultados deverão ser apresentados para a direção, para que sejam tomadas as decisões que influenciarão na fase seguinte;
- *Act* (agir): Essa fase irá buscar a melhoria contínua do SGSI, através da implementação de melhorias, ações corretivas e preventivas, a partir dos resultados obtidos na fase anterior.

A norma está atrelada às ABNT NBR ISO 9001:2000 (norma que trata sobre sistema de gestão da qualidade) e ABNT NBR ISO 14001:2004 (norma que busca estabelecer um sistema de gestão ambiental) para embasamento na implementação e operação consistente e integrada das normas de gestão. Um sistema de gestão corretamente arquitetado pode, dessa forma, preencher os requisitos de todas estas normas [ABNT NBR ISO/IEC 27001, 2006].

A ABNT NBR ISO/IEC 27002, publicada inicialmente como ABNT NBR ISO/IEC 17799, é uma tradução da ISO/IEC 27002.

A ISO/IEC 27002 é um código de prática de SI, ou seja, "um guia prático para desenvolver os procedimentos de segurança da informação da organização e as eficientes práticas de gestão da segurança" [ABNT NBR ISO/IEC 27002, 2005].

A ISO/IEC 27002 possui 15 capítulos, incluindo 133 controles que estão divididos em 11 capítulos, chamados seções de controles de segurança da informação. Há também um capítulo que é uma seção introdutória, que aborda análise, avaliação e tratamento de riscos.

Patricia Peck, em seu livro Direito Digital (2010), diz que, segundo a ISO/IEC 27002, para a implantação da SI são necessários os seguintes passos:

- Inventariar os ativos;
- Realizar análise de risco;
- Classificar as informações;
- Criar um Comitê de Segurança;
- Elaborar uma PSI;
- Auditar os controles que foram criados ou não;
- Criar planos de contingência.

A autora ainda acrescenta que diversos fatores devem ser levados em consideração, como por exemplo, aspectos técnicos (hardware e software para SI) e aspectos jurídicos [PINHEIRO, 2010].

Vale salientar que a ISO/IEC 27002 aconselha a criação das suas próprias diretrizes, pois nem todos os controles da norma podem ser aplicados à sua organização, e também controles adicionais (não incluídos na norma) podem ser necessários.

As normas ISO/IEC 27001 e ISO/IEC 27002 diferem basicamente nos seus objetivos. Cada uma tem um foco específico, mas a aplicação é semelhante, visto que ambas utilizam o mesmo conjunto de controles de SI. As seções de controles listadas no Anexo A da ISO/IEC 27001 são esmiuçadas e detalhadas na ISO/IEC 27002, e a própria ISO/IEC 27001 sinaliza isso, dizendo que os controles são derivados diretamente e estão alinhados com os listados pela ISO/IEC 27002, e que esta "fornece recomendações e um guia de implementação das melhores práticas para apoiar os controles especificados" [ABNT NBR ISO/IEC 27001, 2006].

Logo, para a aplicação da ISO/IEC 27001 é fundamental que a ISO/IEC 27002 seja utilizada em conjunto, possibilitando um melhor entendimento dos controles de SI e uma correta implementação do SGSI.

3.4 Aplicação das Normas

A aplicação do trabalho ocorreu numa indústria do ramo alimentício que teve sua constituição no ano de 1979. A empresa atende principalmente ao estado da Bahia, mas também vende a estados do Sudeste e a outros estados do Nordeste.

Como possui mais de 100 e menos de 500 funcionários, se enquadra como empresa de médio porte, segundo critério de classificação do Instituto Brasileiro de Geografia e Estatística (IBGE) e do Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE) [SEBRAE-SC].

Por se tratar de um trabalho que abordará falhas, vulnerabilidades e outras particularidades de segurança da empresa, convencionou-se que, nesta pesquisa, a mesma será chamada apenas de Empresa.

3.5 Escopo do Trabalho

O trabalho foi realizado no ambiente de Tecnologia, Informação e Comunicação (TIC) da Empresa, ou seja, em seus escritórios. Ali se localizam todos os computadores e periféricos computacionais, por onde transitam todas as informações da organização.

Segundo a nomenclatura utilizada na Empresa, as áreas analisadas foram: Gerência Administrativa, Gerência Comercial, Gerência Financeira, Recursos Humanos, Supervisão de Vendas, Setor Fiscal, Faturamento, Contabilidade, Recepção e o Centro de Processamento de Dados (CPD).

4. Metodologia

Este é um estudo de natureza aplicada, de abordagem quantitativa e qualitativa, que utilizou o método exploratório-descritivo e teve como delineamento o levantamento de dados através do método *survey*.

Os sujeitos da pesquisa foram os diretores e funcionários que faziam parte do fluxo da informação na empresa. Pode ser classificada ainda como uma pesquisa-ação, pois procurou estabelecer uma relação com uma ação ou um problema coletivo.

4.1 Etapas realizadas

As atividades realizadas, em ordem de execução, foram as seguintes:

1. Alinhamento e planejamento de Segurança da Informação;
2. Levantamento tecnológico;

3.Diagnóstico inicial de conformidade;
4.Criação da Política de Segurança da Informação;
5.Criação de documentos auxiliares;
6.Treinamento em Segurança da Informação;
7.Diagnóstico final de conformidade;
8.Pesquisa de satisfação.

4.2 Alinhamento e Planejamento de Segurança da Informação

Antes de iniciar as ações para aplicação das normas, foram necessárias algumas reuniões com a diretoria da Empresa, para que fosse definido o escopo da aplicação, os objetivos da empresa, de modo que tudo fosse feito de forma alinhada aos objetivos de negócio da Empresa.

Na primeira reunião, ocorrida em março de 2011, obteve-se o comprometimento da diretoria no desenvolvimento do trabalho, onde, a partir da proposta realizada, foi possível contar com o apoio para a disponibilização dos recursos (tempo, pessoas e equipamentos), dentro dos limites que a própria diretoria iria definir ao longo do trabalho.

O próximo passo foi alinhar as opiniões e objetivos, para realizar o trabalho de acordo com o que a Empresa mais precisava no que diz respeito à SI. Para isso aconteceram três reuniões, onde foram discutidos alguns assuntos de forma mais detalhada: quais os objetivos do trabalho, o que as normas utilizadas (ISO/IEC 27001 e ISO/IEC 27002) recomendavam, o que poderia ser aplicado na Empresa, quais os processos críticos da Empresa e as principais ameaças a esses processos.

A partir disso criou-se o planejamento de SI da Empresa, que resultou nas demais atividades.

4.3 Levantamento Tecnológico

Foi realizado um levantamento tecnológico, com o objetivo de oferecer para a organização um maior controle sobre seus recursos tecnológicos e agilidade nas tomadas de decisões que envolvem os recursos de TI. Para tanto, foi documentado todo o ambiente físico e lógico da TI da empresa.

Nesse levantamento foram verificados os seguintes itens:

- Inventário de hardware, que incluiu todos os computadores, incluindo os servidores, impressoras e outros periféricos, assim como suas devidas configurações;
- Inventário de software, com uma lista de todos os softwares instalados em todos os computadores;
- Endereçamento IP, com uma lista dos IPs de todos os computadores;
- Internet, com as configurações e descrições da Internet principal e da Internet que serve de contingência.

Os inventários e listas foram divididos pelos setores da empresa.

4.4 Diagnóstico Inicial de Conformidade

Após o levantamento tecnológico, foram criadas *checklists*. O objetivo era apontar quais requisitos das normas ISO/IEC 27001 e ISO/IEC 27002 estavam sendo atendidos pela Empresa.

As *checklists* foram divididas em: Aspectos Organizacionais, Segurança física, Segurança Lógica, Planos de Contingência.

O método adotado na aplicação das *checklists* consiste numa série de itens relacionados à segurança da informação, onde, para cada item há dois valores. O primeiro valor é uma nota que varia de zero a 10 e aponta a situação na qual a empresa se encontra, sendo zero o item totalmente inexistente e 10 o item que é completamente implementado, em perfeito estado. O segundo valor é o grau de importância atribuído para o item, que deve receber um dos seguintes valores:

- um, quando o item não for importante;
- cinco, quando o item tiver média importância;
- dez, quando o item tiver alta importância.

Com os *checklists* respondidos, realizou-se o seguinte cálculo: em cada item multiplicou-se a nota pelo grau de importância atribuído, e em seguida o resultado da soma de todos os itens foi dividido pela quantidade de itens, apurando-se a média geral.

4.5 Criação da Política de Segurança da Informação

Uma das principais atividades no processo de implementação das normas ISO/IEC 27001 e ISO/IEC 27002 é a criação da PSI. Essa atividade foi uma das mais demoradas (levou aproximadamente três meses para ser realizada), pois dependia de alinhamento com a diretoria e aceitação das diretrizes que iriam compor a política.

As maiores dificuldades do trabalho foram identificadas durante a criação da PSI. A primeira diz respeito ao entendimento e conhecimento sobre SI. Em cada etapa ou assunto, fora necessário explicar várias vezes os conceitos e objetivos para que fossem compreendidos e aceitos. A segunda dificuldade foi com relação ao tempo e esforço, dedicados. Apesar da demonstração de interesse dos diretores, revelou-se tarefa árdua realizar reuniões com a diretoria. Muitas vezes participavam apenas um ou dois dos diretores, e diversas vezes reuniões foram adiadas por motivos variados, o que atrasou a realização das atividades.

Possíveis ameaças foram expostas e as diretrizes foram alinhadas. Com relação ao custo, todo o trabalho realizado foi isento de custos para a Empresa. Porém, houve gastos para que fossem colocados em prática os Planos de Continuidade, objetivando a não interrupção de atividades críticas como, por exemplo, os montantes despendidos com a aquisição de um servidor secundário (reserva). Também houve gastos indiretos relativos ao tempo disponibilizado, principalmente pela diretoria. Destarte, os gastos foram mínimos, sempre abaixo do máximo estipulado pela diretoria da Empresa.

A diretoria também tinha algumas preocupações prévias, relativas à: criação de senhas; proliferação de códigos maliciosos; realização de *backups*; e interrupção de atividades críticas.

Essas preocupações foram avaliadas e diretrizes foram criadas na PSI para regulamentar procedimentos, no sentido de reduzir os riscos ou impactos das possíveis ameaças.

Após total alinhamento das diretrizes e permissão da diretoria, a PSI foi finalizada e apresentada aos diretores e aos funcionários.

4.6 Criação de documentos auxiliares

Alguns documentos foram criados para dar apoio à PSI e, consequentemente, ao SGSI da Empresa.

Inicialmente, criou-se um documento chamado “Declaração de Comprometimento”, que tem como objetivo atestar a aprovação da PSI e o comprometimento da diretoria da empresa no cumprimento da mesma, seguindo os prazos estabelecidos, disponibilizando os recursos necessários, cobrando e conscientizando os funcionários etc. Em seguida, foram criados os seguintes documentos: Comitê Permanente de Segurança (CPS) e Grupo de Segurança de Informação (GSI).

Para atender a algumas necessidades apontadas pela empresa, foram criadas algumas Normas de SI. São elas: “Uso da Internet”, “Uso do e-mail”, “Uso da senha de acesso”.

Também foi criado o “Formulário de registro de Incidente de Segurança”, com o objetivo de documentar os incidentes de segurança de informação, possibilitando investigações posteriores e ações corretivas mais eficientes.

Posteriormente, foi criado também um "Termo de Responsabilidade e Sigilo", no intuito de dar um subsídio legal para a Empresa cobrar o compromisso dos funcionários, no que diz respeito a: seguir as políticas e normas, reconhecer a Empresa como proprietária das informações inerentes a ela, manter o sigilo das informações e ter ciência de que suas ações podem ser monitoradas pela empresa.

Por fim, foi criado o documento intitulado "Planos de continuidade de negócios", que consta de três planos de continuidade, para atender aos recursos ou serviços mais críticos (de maior impacto na ocorrência de incidentes) da Empresa.

4.7 Treinamento em Segurança da Informação

Funcionários e diretores da empresa participaram do treinamento em SI. O treinamento objetivava conscientizá-los e treiná-los nas boas práticas de SI, mas foi utilizado também como instrumento para apresentar a PSI, as normas e os procedimentos criados, os objetivos do trabalho e o apoio da diretoria. Essa atividade durou aproximadamente dois meses, pois demandava tempo dos participantes e, portanto, era necessário aguardar que estivessem disponíveis.

O treinamento dividiu-se em três partes, e foi realizado com grupos de três ou quatro pessoas, por vez. De acordo com a disponibilidade dos presentes, eram apresentadas uma, duas ou até as três partes do treinamento em um mesmo dia.

A primeira parte foi introdutória e tratou de: conceitos básicos; conscientização, justificando a importância de se preocupar com a SI e mostrando a situação atual da SI no Brasil e na Empresa; apresentação dos objetivos do trabalho; e comprometimento da diretoria na realização do mesmo.

Na segunda parte foram apresentados alguns problemas típicos de SI nas organizações, dificuldades para a conscientização, exemplos de casos e situações reais, direitos e deveres dos funcionários, alguns conceitos relacionados a códigos maliciosos e foram recomendadas cartilhas gratuitas que tratam o tema segurança.

Na terceira e última parte do treinamento foram apresentadas: dicas gerais e boas práticas de SI; as normas que foram criadas para dar apoio à PSI; dicas relativas a transações bancárias pela Internet, como lidar com o spam, cuidados com dispositivos móveis e com códigos maliciosos. Em seguida, passou-se à parte prática do treinamento, onde todos aprenderam a: como criar senhas mais seguras, como identificar sites e e-mails falsos; como utilizar o antivírus corporativo para remover ameaças detectadas, realizar atualizações e verificações manuais, e como reportar a detecção de ameaças pelo antivírus.

4.8 Diagnóstico Final de Conformidade

A partir das mesmas *checklists* utilizadas anteriormente, no Diagnóstico inicial de conformidade, foi feito um novo diagnóstico de conformidade, utilizando o mesmo método. Para cada item foram mantidos os graus de importância atribuídos anteriormente, mas foram inseridas novas notas para a situação. Em seguida calculou-se a média geral, para comparação com o diagnóstico inicial de conformidade.

4.9 Pesquisa de satisfação

Ao final do trabalho, foi realizada uma pesquisa de satisfação com funcionários e com diretores da empresa. O objetivo da pesquisa foi mensurar o que os diretores e funcionários pensavam sobre o trabalho realizado e o seu impacto no dia a dia da empresa.

Para a realização da pesquisa fez-se necessário submeter o projeto a apreciação do Comitê de Ética em Pesquisa (CEP) da Universidade Estadual do Sudoeste da Bahia (UESB). O procedimento

para coleta de dados teve início tão logo foi aprovado e autorizado pelo CEP, conforme o Certificado de Apresentação para Apreciação Ética (CAAE) número 03619112.7.0000.0055.

Todos os participantes tiveram que assinar um Termo de Consentimento Livre e Esclarecido (TCLE), o qual esclarece os objetivos da pesquisa, além dos direitos do participante e dos pesquisadores.

A pesquisa foi dividida em dois questionários, um a ser respondido pelos diretores e o outro pelos demais funcionários. Cada um deles, contendo perguntas em comum e perguntas específicas. No total, foram três questionários respondidos pelos diretores e oito respondidos pelos funcionários.

Após aceitar participar da pesquisa e assinar o TCLE, o funcionário ou diretor pôde responder a pesquisa.

Em seguida as respostas dos questionários foram contabilizadas e tabeladas, para a obtenção dos resultados.

5. RESULTADOS

Os resultados obtidos no Diagnóstico inicial de conformidade foram:

- Aspectos Organizacionais: 25,51%;
- Segurança Física: 54,66%;
- Segurança Lógica: 49,54%;
- Planos de Contingência: 28,40%.

Os resultados obtidos no Diagnóstico final de conformidade foram:

- Aspectos Organizacionais: 75,83%;
- Segurança Física: 66,70%;
- Segurança Lógica: 71,52%;
- Planos de Contingência: 78,26%.

A Figura 4 traz um gráfico com o comparativo dos diagnósticos inicial (1º diagnóstico) e final (2º diagnóstico).

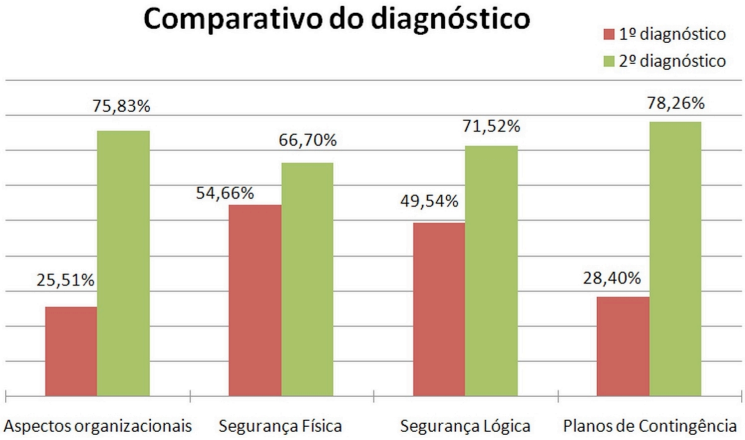

Figura 4. Comparativo do diagnóstico

É notável que dois itens de SI tiveram grande melhoria (aproximadamente 50%) e outros dois itens tiveram melhoria inferior a 25%.

Os resultados da checklist de aspectos organizacionais tiveram grande melhoria, devido à criação da PSI, e normas e procedimentos implantados em decorrência da mesma.

Em decorrência da criação dos planos de continuidade para serviços críticos, o diagnóstico dos planos de contingência também apresentou grande melhoria nos resultados.

Os itens segurança física e segurança lógica tiveram uma melhoria inferior, que ocorreu devido a dois motivos principais: ambos tinham 50% ou mais de conformidade; ambos necessitavam de um maior investimento financeiro para melhorias mais significativas.

Comparando-se os resultados, a melhoria do 1º para o 2º diagnóstico foi de: 50,32% em Aspectos Organizacionais, 12,04% em Segurança Física, 21,98% em Segurança Lógica e 49,86% em Planos de Contingência.

Os resultados da pesquisa de satisfação apresentados em 28 gráficos. Sendo 18 dos questionários aplicados com a diretoria e 10 com os funcionários.

A Figura 5 ilustra alguns dos resultados dos questionários aplicados com a diretoria.

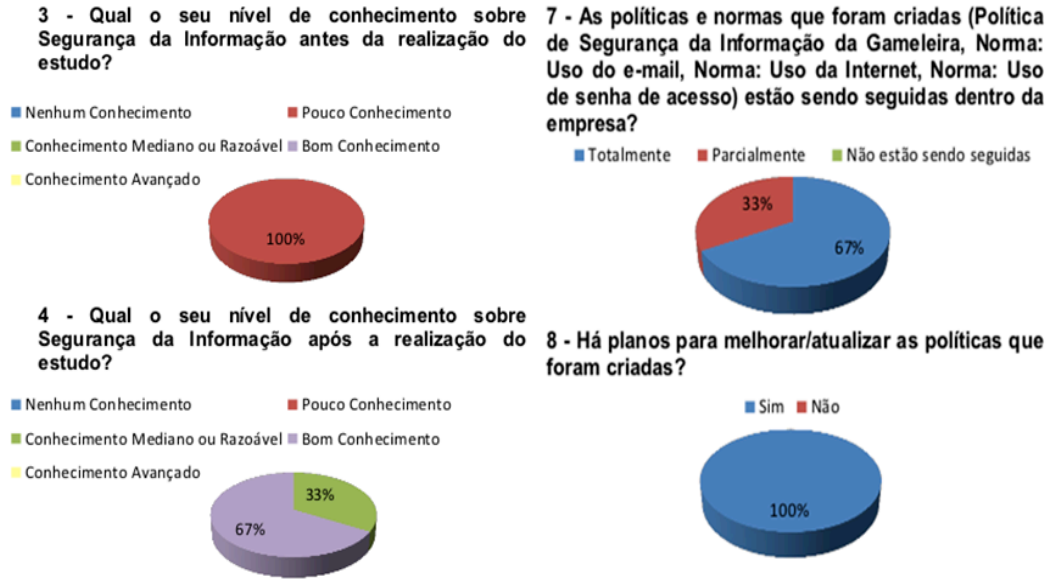

Figura 5. Gráficos diretoria 1

Como visto na Figura 5, os participantes consideraram que tiveram uma boa melhoria em seus conhecimentos sobre SI e a maioria respondeu que as políticas e normas que foram criadas estão sendo seguidas e que há planos para que sejam atualizadas.

As perguntas 11 e 12 (Figura 6) abordam os planos de continuidade. Os diretores da Empresa responderam que alguns planos já foram testados e que já houve a necessidade de utilização. Ainda na Figura 6, sobre o número de incidentes de segurança, todos os participantes afirmam que houve alta redução, e sobre custos, a maioria dos diretores acredita que a Empresa teve custos durante o estudo.

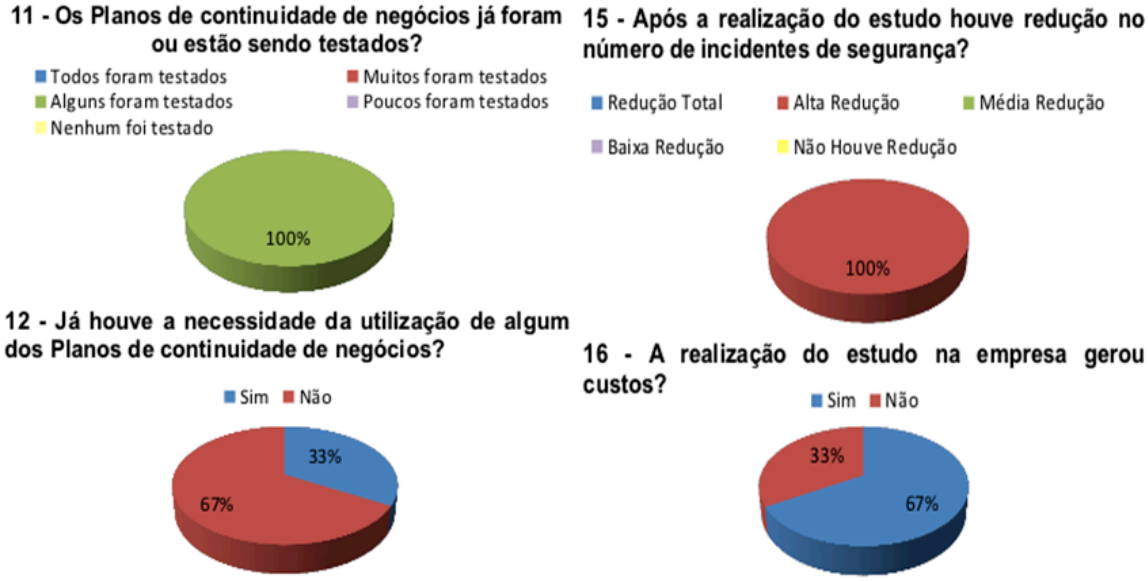

Figura 6. Gráficos diretoria 2

A alguns dos resultados dos questionários aplicados com os funcionários.

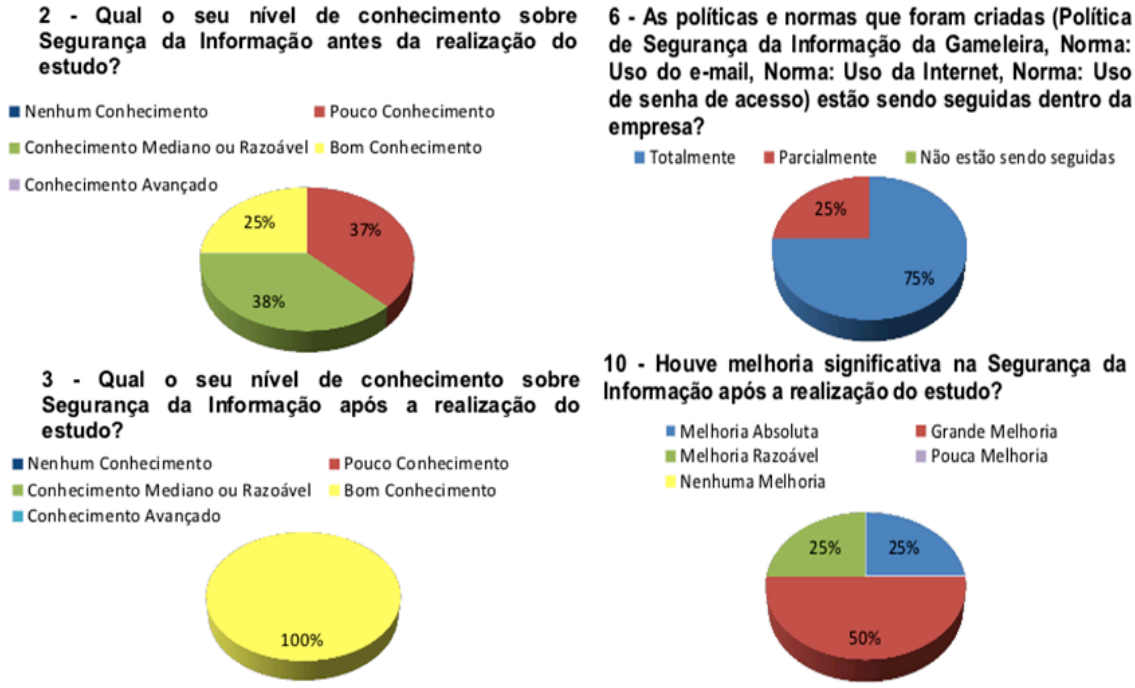

Figura 7. Gráficos funcionários

Como visto na Figura 7, a maioria dos participantes considerou que o seu nível de conhecimento sobre SI melhorou. A pergunta 6 questionou sobre as políticas e normas que foram criadas. A maioria dos participantes respondeu que as mesmas estão sendo seguidas totalmente, enquanto 25% afirmou que são seguidas parcialmente. Na pergunta 10, ainda na Figura 7, é possível observar que todos os participantes consideraram que houve melhoria na SI da empresa, onde 50% afirmaram ter havido grande melhoria.

6. CONCLUSÃO

Para a realização deste trabalho, foi levada em consideração a rápida evolução tecnológica, o aumento crescente no número de crimes digitais e incidentes de segurança, como também a situação atual da Segurança da Informação no âmbito corporativo.

Após a aplicação das normas ISO/IEC 27001 e ISO/IEC 27002 foi possível observar uma grande melhoria nos níveis de SI da empresa. O resultado do diagnóstico de conformidade final mostrou uma melhoria significativa e o resultado da pesquisa de satisfação mostrou que funcionários e diretores ficaram mais satisfeitos com o desempenho do trabalho.

A partir dos resultados obtidos neste trabalho, pôde-se chegar à conclusão de que é possível melhorar os índices de Segurança da Informação na empresa com baixo custo, e ainda que normas de gestão de SI podem ser aplicadas com sucesso em empresas de médio porte.

7. Referências

ABNT NBR 15999-1. (2007). *Gestão de continuidade de negócios. Parte 1: Código de prática*. Rio de Janeiro: Associação Brasileira de Normas Técnicas.

ABNT NBR 15999-2. (2008). *Gestão de continuidade de negócios Parte 2: Requisitos*. Rio de Janeiro: Associação Brasileira de Normas Técnicas.

ABNT NBR ISO/IEC 27001. (2006). *Tecnologia da informação – Técnicas de Segurança – Sistemas de gestão de segurança da informação – Requisitos*. Rio de Janeiro: Associação Brasileira de Normas Técnicas.

ABNT NBR ISO/IEC 27002. (2005). *Tecnologia da informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação*. Rio de Janeiro: Associação Brasileira de Normas Técnicas.

ABNT NBR ISO/IEC 27003. (2011). *Tecnologia da informação – Técnicas de Segurança – Diretrizes para implantação de um sistema de gestão da segurança da informação*. Rio de Janeiro: Associação Brasileira de Normas Técnicas.

ABNT NBR ISO/IEC 27004. (2010). *Tecnologia da informação – Técnicas de Segurança – Gestão da segurança da informação — Medição*. Rio de Janeiro: Associação Brasileira de Normas Técnicas.

ABNT NBR ISO/IEC 27005. (2008). *Tecnologia da informação – Técnicas de Segurança – Gestão de riscos de segurança da informação*. Rio de Janeiro: Associação Brasileira de Normas Técnicas.

ÂNGELO, F. (2009). *Segurança deve ser foco de pequenas e médias empresas*. COMPUTERWORLD, http://computerworld.uol.com.br/seguranca/2009/10/27/pequenas-e-medias-empresas-tambem-devem-focar-em-seguranca/, Julho de 2012.

British Standard (BS). (2006). *BS 7799-3:2006*. http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030125022, Dezembro de 2012.

CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil). (2014). *inc-stats.png*. http://www.cert.br/stats/incidentes/inc-stats.png, Fevereiro de 2014.

CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil). (2012). *Sobre o CERT.br.* http://www.cert.br/sobre/, Janeiro de 2014.

ISO (International Organization for Standardization). (1999). *ISO/IEC 15408-1:1999. Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*. Genebra.

ISO (International Organization for Standardization). (2012). *ISO/IEC 27000:2012. Information technology — Security techniques — Information security management systems — Overview and vocabular*. Genebra.

ISO (International Organization for Standardization). (2011). *ISO/IEC 27006:2011*. http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=59144, Fevereiro de 2013.

MORAZ, E. (2006). *Treinamento Profissional Anti-Hacker*. 1. ed. São Paulo: Digerati Books.

PINHEIRO, P. P. (2010). *Direito Digital*. 4. ed. São Paulo: Saraiva.

Profissionais de TI. (2010). *PDCA_SGSI.jpg*. http://www.profissionaisti.com.br/wp-content/uploads/2010/10/PDCA_SGSI.jpg, Janeiro de 2013.

RAMOS, A. (2008). *Security Officer – 1: guia oficial para formação de gestores em segurança da informação*. Módulo Security Solutions 2.ed. Porto Alegre: Zouk.

SEBRAE-SC. (2013). *Critérios de classificação de empresas: EI – ME – EPP*. http://www.sebrae-sc.com.br/leis/default.asp?vcdtexto=4154, Fevereiro de 2013.

The ISO 27000 Directory. (2013). *A Short History of the ISO 27000 Standards*. http://www.27000.org/thepast.htm, Fevereiro de 2013.

WOOD, M. B. (1984). *Introdução à segurança do computador*. Rio de Janeiro. Editora Campus.