UNIVERSIDADE ESTADUAL DE MATO GROSSO DO SUL
UNIDADE UNIVERSITÁRIA DE MARACAJU
CURSO DE ADMINISTRAÇÃO

ROSEMIR DE JESUS VILIAHAR

ANÁLISE DA UTILIZAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO EM UM ESCRITÓRIO DE CONTABILIDADE EM MARACAJU/MS

MARACAJU - MS

2016

UNIVERSIDADE ESTADUAL DE MATO GROSSO DO SUL
UNIDADE UNIVERSITÁRIA DE MARACAJU
CURSO DE ADMINISTRAÇÃO

ROSEMIR DE JESUS VILIAHAR

ANÁLISE DA UTILIZAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO EM UM ESCRITÓRIO DE CONTABILIDADE EM MARACAJU/MS

Monografia apresentada à Universidade Estadual de Mato Grosso do Sul (UEMS), como exigência do Curso de Administração sob orientação do Professor Wilson Correa da Silva.

MARACAJU - MS

2016

UNIVERSIDADE ESTADUAL DE MATO GROSSO DO SUL

UNIDADE UNIVERSITÁRIA DE MARACAJU
CURSO DE ADMINISTRAÇÃO

REITOR

PROF. DR. FÁBIO EDIR DOS SANTOS COSTA

PRÓ-REITOR DE ENSINO

PROF. DR. JOÃO MIANUTTI

COORDENADOR DE CURSO

PROF. DR. ALEX SANDRO RICHTER WON MÜHLEN

ORIENTADOR

PROF. ADM. WILSON CORREA DA SILVA

A monografia intitulada “ANÁLISE DA UTILIZAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO EM UM ESCRITÓRIO DE CONTABILIDADE EM MARACAJU/MS”, apresentada por Rosemir de Jesus Viliahar, como exigência parcial para obtenção do grau Bacharel em Administração da UEMS Universidade Estadual de Mato Grosso do Sul – Unidade de Maracaju, foi aprovada.

Maracaju MS, 17 de novembro de 2016.

BANCA EXAMINADORA

Prof. Adm. Wilson Correa da Silva (Orientador)

Prof. Dr. Ulisses Simon da Silveira

Prof. Dr. Alex Sandro Richter Won Mühlen

DEDICATÓRIA

de modo especial, à minha esposa Daiane, fonte de incentivo e apoio em todos os momentos.

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus, pois sem ele nada é possível. Agradeço pela minha vida, minha família, meus amigos e por mais esta realização.

A minha mãe *Maria Eliza de Jesus Viliahar*, que apesar das dificuldades enfrentadas, sempre incentivou meus estudos.

A minha esposa *Daiane de Arruda Costa Viliahar*, que foi a pessoa que mais me apoiou e me incentivou a estudar.

A todos os Professores do curso de Administração e em especial ao *Prof. Adm. Wilson Correa da Silva* pela sua orientação, pela sua disponibilidade e por toda sua ajuda na realização deste trabalho e ao *Prof. Me. Moysés Simão Kaveski* que jamais deixou de me incentivar.

EPÍGRAFE

Tente uma, duas, três vezes e se possível tente a quarta, a quinta e quantas vezes for necessário. Só não desista nas primeiras tentativas, a persistência é amiga da conquista. Se você quer chegar à onde a maioria não chega, faça o que a maioria não faz.

Bill Gates

RESUMO

Este trabalho aborda uma análise da utilização de uma Política de Segurança da Informação: um estudo de caso em um escritório de Contabilidade em Maracaju/MS. O objetivo consistiu em analisar se os procedimentos de proteção das Informações utilizados pela organização pesquisada estão de acordo com a norma ISO/IEC 27002:2013, para garantir que as informações produzidas dentro da empresa sejam armazenadas e tratadas com segurança, garantindo assim sua confiabilidade. Foi aplicada uma pesquisa de opinião, no qual foram aplicados dois questionários estruturado com perguntas objetivas (questões fechadas), um dirigido a gerencia e o outro a 11 (onze) funcionários envolvidos diretamente na manipulação das informações. Para um melhor entendimento, os resultados dos dois questionários foram analisados e discutidos separadamente e confrontados em seguida. Pelos resultados obtidos observou-se por parte da gerencia, que havia uma norma interna de Segurança da Informação, mas a mesma não está de acordo com a ISO/IEC 27002:2013. Por parte dos funcionários, foi descoberto que a maioria sabe o significado de uma Política de Segurança da Informação, mas nem todos conhecem as normas de segurança da empresa.

Palavras-chave: Informação; Política e Segurança.

SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS

ABNT - Associação Brasileira de Normas Técnicas

CERT.BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

IEC - International Electrotechnical Comission (Comissão Internacional de Eletrotécnica)

ISO - International Organization for Standardization (Organização Internacional para Padronização)

NBR - Norma Brasileira Regulamentadora

PIS - Políticas de Segurança da Informação

SGSI - Sistema de Gestão de Segurança da Informação

SI - Segurança da Informação

SIC - Segurança da Informação e das Comunicações

SSI - Sistema de Segurança da Informação

TI - Tecnologia da Informação

INTRODUÇÃO

Na atualidade, devido aos avanços tecnológicos, a informação se tornou o ativo mais importante para as organizações. As informações são tantas (estratégicas, confidenciais, senhas, dados pessoais, cadastros de clientes, etc.) que necessitam de um cuidado especial. Quem tem informação, tem poder, e é nesse sentido, que diversos procedimentos são adotados constantemente pelas empresas para garantir a confidencialidade, a integridade e a disponibilidade de suas informações.

A informação caminha numa velocidade imensurável, na mesma proporção também surgem as ameaças e vulnerabilidades a esse ativo. Um grande escândalo, uma falha ou uma brecha de segurança podem fechar as portas de qualquer empresa. Atualmente a Segurança da Informação também se desenvolve de forma rápida, fazendo com que as organizações tenham maior eficiência e rapidez nas tomadas de decisão.

À medida que estas informações são disponibilizadas, todos os colaboradores que delas necessitam, devem ser informados de suas responsabilidades perante a segurança e das consequências ao descumprir as normas de segurança.

Mesmo com a contribuição da Segurança da Informação existem empresas que não utilizam uma PSI ou a utiliza de maneira incorreta. Assim podemos afirmar que independentemente do tamanho da empresa ou da quantidade de funcionários que ela possui, todas devem ter sua PSI e todos os membros da organização têm que estar envolvidos diretamente com ela.

1. CONTEXTUALIZAÇÃO E DEFINIÇÃO DA PESQUISA

1.1 Problema

Constantemente as empresas sofrem com inúmeras ameaças em seus sistemas de informações. Através de computadores ligados ou não a internet, sofrem espionagens, sabotagens, fraudes, dentre outros ataques virtuais.

Além das ameaças tecnológicas, pessoas de dentro da organização que desconhecem qualquer tipo de política de segurança da informação, podem vazar dados sigilosos que consequentemente irão resultar na perda de credibilidade e confiabilidade da empresa no mercado.

A informação sem dúvida é o ponto mais vulnerável de uma empresa e a não aceitação do setor administrativo da empresa em protegê-las dificulta e põe em risco a segurança dos dados gerados dentro da organização. Essa aceitação não deve partir apenas da diretoria, mas também de todos os funcionários. Para que a cultura da empresa seja mudada em relação à segurança da informação, é fundamental que os funcionários estejam preparados para a mudança. A falta de conhecimento sobre o assunto ou a mesmice do dia a dia dificulta a criação de métodos mais funcionais e seguros para lidar com a informação.

Sem essa conduta e a falta de algumas regras de segurança pré-estabelecidas, a empresa se torna inconsistente e frágil, podendo apresentar algum tipo de risco aos clientes e a si própria.

Para assegurar total proteção das informações criadas e manipuladas pela empresa e assim prevenir a ocorrência de possíveis incidentes que leve a perda da credibilidade da empresa, surge o seguinte questionamento: A Política de Segurança da Informação utilizada na organização pesquisada está de acordo com a norma ISO/IEC 27002:2013?

1.2 Justificativa

Vivemos em uma sociedade onde as informações se multiplicam notoriamente em questão de segundos, devido a grandes avanços tecnológicos. Os setores empresariais, obviamente, tentam acompanhar essas mudanças, logo, as informações que eram armazenadas apenas em papel, e de fácil acesso, começam a serem arquivadas de forma mais sofisticada com a utilização de computadores, internet, e outros diversos recursos tecnológicos.

Toda essa praticidade que as tecnologias trazem, principalmente ao setor empresarial, pode também gerar muitos problemas relacionados à segurança das Informações, tanto as que são produzidas dentro das organizações, quanto as pertencentes aos clientes. Isso advém,

principalmente de uma falha da empresa em reconhecer que precisa preservar seu principal patrimônio a “Informação”.

A implementação de um conjunto de regras de segurança denominada “Políticas de Segurança da Informação” que esteja em conformidade com a ISO/IEC 27002:2013, ajuda a assegurar a integridade e a disponibilidade das informações na organização, garantindo que as mesmas não sejam alteradas ou perdidas, permitindo assim, que as informações estejam seguras e disponíveis quando necessário.

A falta dessa política ou a sua utilização de maneira errada, implicará na quebra de sigilo da empresa (vazamento de dados), ataques virtuais, que irão gerar problemas com sua reputação e permanência no mercado.

Portanto, esse trabalho se justifica pela necessidade em contribuir para uma melhor gestão organizacional que garanta a integridade, confidencialidade, autenticidade e disponibilidade das informações criadas e ou manipuladas pela organização.

1.3 Hipótese

A preocupação constante de estarem sempre à frente do mercado, as vezes atrapalha muitas empresas em se preocuparem com a segurança de suas Informações e quando se dão conta de sua importância, não sabem por onde começar.

A possível causa para as principais deficiências de Segurança da Informação na organização pesquisada é da não utilização de uma Política de Segurança da Informação que atenda à risca a norma ISO/IEC 27002:2013. Isso se deve à falta de conhecimento dos gestores e dos funcionários a respeito de sua importância dentro e fora do ambiente de trabalho.

Para sanar esse problema, a diretoria teria que dar mais atenção a Segurança da Informação e criar a sua PSI devidamente documentada. E para isso, ela deve contar com a ajuda de todos os funcionários, colaborando uns com os outros e respeitando essa Política de acordo com os valores da organização.

1.4 Objetivos

- Objetivo Geral

Analisar se os procedimentos de proteção as Informações utilizados pela organização pesquisada estão de acordo com a norma ISO/IEC 27002:2013.

- Objetivos Específicos

- Observar a existência de uma Política de Segurança da Informação na empresa.
- Esclarecer sobre a importância de se ter uma boa PSI.
- Constatar se a gerencia e os funcionários possuem total entendimento sobre o significado de uma PSI.
- Verificar se a Política atual da organização possui uma certificação ISO.

2. REVISÃO DE LITERATURA

2.1. Informação

Para entendermos o que é Segurança da Informação e qual a sua importância para as empresas, temos que definir o conceito de Informação. Nesse sentido a ISO/IEC 27002 (2005) descreve a informação como sendo um conjunto de dados que após serem processados torna-se uma informação. Um dado antes de ser processado não possui nenhum valor, a partir do seu processamento, ele passa a ser considerado uma informação com tamanha importância para geração do conhecimento.

Pode-se afirmar então que, a informação é o resultado da análise de dados recebidos ou produzidos. Esses dados depois de processados e separados pelo seu grau de importância tornam-se uma informação.

Filho (2014, p. 04) enfatiza que a:

> Informação compreende qualquer conteúdo que possa ser armazenado ou transferido de algum modo, servindo a determinado propósito e sendo de utilidade ao ser humano. Trata-se de tudo aquilo que permite a aquisição de conhecimento. Nesse sentido, a informação digital é um dos principais, senão o mais importante, produto da era atual. Ela pode ser manipulada e visualizada de diversas maneiras. Assim, à medida que a informação digital circula pelos mais variados ambientes, percorrendo diversos fluxos de trabalho, ela pode ser armazenada para os mais variados fins, possibilitando ela ser lida, modificada ou até mesmo apagada.

Sêmola (2003) pontua que a informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional e saúde da empresa. Possuir Informação é ganhar agilidade, competitividade, previsibilidade, dinamismo. Informação é um diferencial, Informações úteis podem ser usadas a seu favor ou contra você e sua empresa.

Independente da forma que a informação se apresenta ela deve ser protegida de maneira adequada, sendo assim:

> Organizações de todos os tipos e tamanhos (incluindo o setor privado e público, organizações comerciais e sem fins lucrativos), coletam, processam, armazenam e transmitem informações em diferentes formatos, incluindo o eletrônico, físico e verbal (por exemplo, conversações e apresentações). O valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações, são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requer proteção contra vários riscos. (NBR ISO/IEC 27002, 2013, p. 04)

Fazer um uso efetivo da informação permite que uma organização aumente a eficiência de suas operações, o que representa um diferencial competitivo em relação aos

concorrentes, para tanto, é necessário o reconhecimento das empresas em admitir que a Informação precisa de maiores cuidados.

2.1.1. Tipos de Informação

A classificação da informação de acordo com o seu valor para a empresa contribui para a manutenção das suas principais características de segurança que são: a integridade; a disponibilidade e a confidencialidade.

A ABNT NBR ISO/IEC 27002 (2013) não estabelece um padrão de classificação para as informações, mas recomenda que elas sejam classificadas de acordo com o seu valor, requisitos legais, sensibilidade e criticidade para a organização e assim assegurar que a informação receba um nível adequado de proteção. Já para Laureano e Morais (2005), as empresas devem classificar suas informações em pública, interna, confidencial e secreta, como descrito abaixo:

- Pública: a informação depois de um certo tempo, pode ser exposta ao público sem que cause consequências danosas a empresa;
- Interna: o acesso a esse tipo de informação deve ser limitado, embora as consequências do uso não autorizado não sejam tão sérias. Sua integridade é importante, mesmo que não seja vital;
- Confidencial: informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente, perdas financeiras, ou de confiabilidade perante o cliente externo, além de permitir vantagem expressiva ao concorrente;
- Secreta: informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito apenas a gerencia. O uso desse tipo de informação é vital para a organização e não pode ser levada a público.

2.1.2. Ciclo de Vida da Informação

Todo e qualquer momento vivido por uma informação, até mesmo situações de riscos, é denominado de Ciclo de Vida da Informação. Um dado é gerado, permanece disponível pelo tempo necessário, passa por atualizações e depois ao perder sua utilidade deve ser descartada adequadamente. Mas dentre todo esse processo Laureano e Morais (2005) pontua que existem quatro momentos que devem ser merecedores de atenção, pois correspondem às situações onde a informação é exposta a ameaças colocando em risco sua integridade, disponibilidade e confidencialidade. Esse ciclo é demonstrado na figura 01.

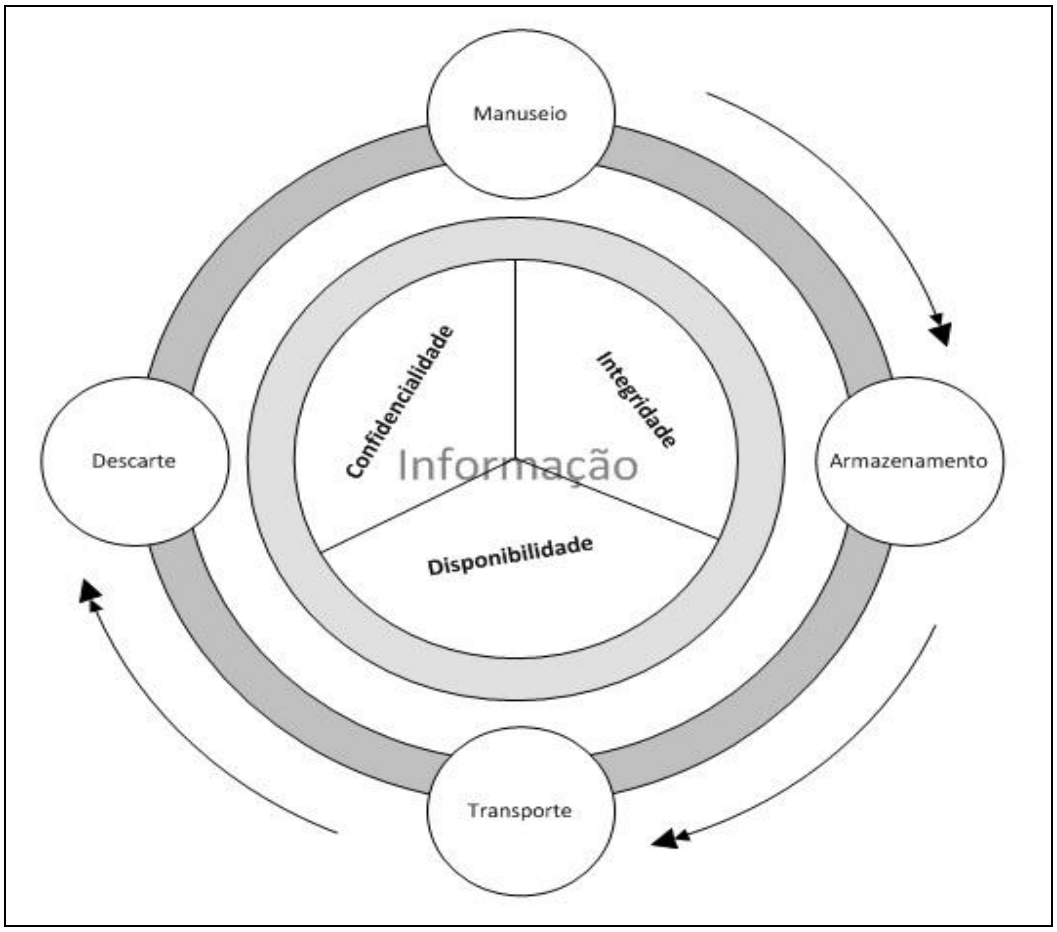

Figura 01: Ciclo de vida da Informação.
Fonte: Laureano e Morais (2005).

- **Manuseio:** trata-se do momento em que a Informação é criada ou manipulada;
- **Armazenamento:** refere-se ao local e a forma que a Informação é armazenada;
- **Transporte:** abrange todos os meios de transporte possível para uma Informação (fax, e-mail, correios, entrega via transportadora, etc.)
- **Descarte:** é o lugar e o procedimento adotado para dar fim a uma Informação que já não é mais útil para a empresa.

Partindo do mesmo princípio de Laureano e Morais (2005) a NBR ISO/IEC 27002 (2013) exemplifica o ciclo de vida da informação e alerta sobre a importância da segurança em todos os seus processos.

> A informação tem um ciclo de vida natural, desde a sua criação e origem, armazenagem, processamento, uso e transmissão, até a sua eventual destruição ou obsolescência. O valor e os riscos aos ativos podem variar durante o tempo de vida da informação (por exemplo, revelação não autorizada ou roubo de balanços financeiros de uma companhia, é muito menos importante depois que elas são formalmente publicadas), porém a segurança da informação permanece importante em algumas etapas de todos os estágios. (NBR ISO/IEC 27002, 2013, p. 06)

Compreender e gerenciar o Ciclo de Vida da Informação é uma tarefa complexa, pois ainda não existem sistemas e modelos definitivos, mas a preocupação constante dos Gestores com a segurança da Informação é essencial para esse desafio. Além disso, a classificação da Informação de acordo com o seu valor é essencial para o bom funcionamento dos negócios da organização.

2.1.3. Ameaças a Informação

De acordo com o dicionário Houaiss (2009), ameaça significa: "Indício de acontecimentos desfavorável ou maléfico". Com o imenso volume de informações produzidas diariamente e tendo em mente o seu alto valor, surgem a todo momento inúmeros tipos de ameaças.

Para Nascimento (2014) (apud Laudon e Laudon, 1999), as principais ameaças aos sistemas de informação computadorizados são catástrofes, falhas elétricas, mau funcionamento de equipamentos, erros de software e mau uso de computador pelo próprio usuário.

Quase sempre uma ameaça surge através de um incidente. Segundo a CERT.BR (2012, p. 50), "um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança de sistemas de computação ou de redes de computadores".

CERT.BR (2012) relata que, tentativa de acesso não autorizado, tentativa de tornar serviços indisponíveis, modificação nos Sistemas de Informação (sem o conhecimento ou consentimento prévio dos donos) e o desrespeito a PSI ou a outra Política de uma instituição, são exemplos de incidentes de segurança. É muito importante que as empresas notifiquem ao Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.BR) sempre que se deparar com uma atitude que considere abusiva ou com um incidente de segurança. Ao notificar um incidente, além de se proteger e contribuir para a segurança global da Internet, também ajudar outras empresas a detectarem problemas, como computadores infectados, falhas de configuração e violações em PSI.

De acordo com a Figura 02, podemos observar os incidentes reportados por empresas situadas no Brasil ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR), no período de 1999 a 2015. Nela podemos observar o crescimento de relatos de incidentes que ocorreram, principalmente em 2014, isso pode ser pelo uso mais

intenso de Sistemas de Informação computadorizados ou pela preocupação das empresas com a segurança.

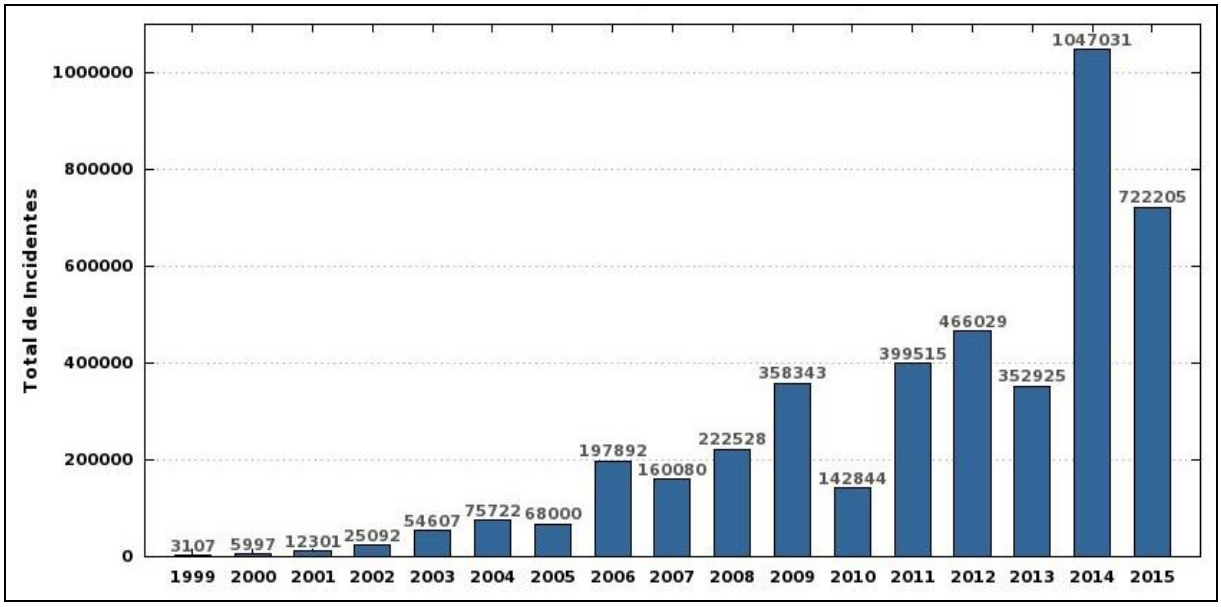

Figura 02: Total de incidentes relacionados à Segurança da Informação reportados ao CERT.BR por ano.
Fonte: CERT.BR. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em 13/07/2016.

Netto e Silveira (2007) descrevem que para um melhor entendimento dos tipos de ameaças, a Segurança da Informação foi dividida em três camadas: física; lógica e humana. Em cada uma dessas camadas deve-se verificar quais os tipos de ameaças que estão presentes ou possíveis de se adquirir e também os métodos de proteção e prevenção para cada uma delas.

2.1.3.1. Camada Física

De acordo com Netto e Silveira (2007), a camada física nada mais é que o ambiente onde está fisicamente instalado os equipamentos utilizados nas empresas. Todo e qualquer equipamento, seja eletrônico ou não, está sujeito a falhas técnicas, é por esse motivo que as empresas devem ficar alertas a respeito da vida útil e da sua manutenção preventiva, para que assim não venha a ter surpresas desagradáveis.

Segundo Turban, et. al. (2010), a segurança da camada física refere-se à proteção de instalações e recursos de informática, incluindo a proteção das propriedades físicas como computadores, servidores, centros de dados e redes.

A segurança da camada física também fornece vários tipos de controles como: proteção contra campos magnéticos; interrupção de energia de emergência e baterias de backup; alarmes de detecção de movimentos que detectam invasão física, etc. Tudo isso

porque a camada física é a primeira camada de segurança de uma organização e por esse motivo ela deve estar pronta para impedir qualquer tentativa de violação contra a Informação.

2.1.3.2. Camada Lógica

A camada Lógica na interpretação de Turban, et. al. (2010), consiste na parte lógica dos equipamentos, ou seja, todo o Sistema de Informação da empresa, exemplos disso são os: programas, arquivos de computador, plataformas web, internet, etc.

Softwares desatualizados, falta de regras de segurança na internet, senhas fracas, com a junção de tudo isso temos um Sistema de Informação totalmente vulnerável a quebras de sigilos, roubos, fraudes e todos os tipos de ataques à informação. Por isso a recomendação de Araújo e Ferreira (2008) para que as políticas de segurança possuam pelo menos os seguintes procedimentos: uso obrigatório de software antivírus em todos os computadores (principalmente no servidor) e a atualização periódica do banco de dados de vírus; verificação de todo arquivo recebido via internet, pelo software antivírus e treinamento adequado que oriente os usuários para melhor utilização do mesmo.

2.1.3.3. Camada Humana

Por sua vez a camada humana se refere as pessoas que manipulam as informações, sendo assim essa camada necessita receber mais atenção do que as outras. Nascimento (2014) enfatiza que mesmo existindo diversas tecnologias destinadas à proteção dos ativos de informação, o elemento humano é a peça fundamental para que a Política de Segurança da Informação seja implementada de forma eficaz. Ainda segundo Nascimento (2014), os funcionários que não praticam a Segurança da Informação, se tornam os elos mais fracos da empresa, colocando em risco todo o seu patrimônio.

Antigamente, a atenção da segurança da informação estava focada apenas para a tecnologia. Hoje, Rezende e Abreu (2000) destaca que, as empresas estão procurando dar mais atenção as pessoas, pois são elas que fazem as empresas funcionarem perfeitamente e em harmonia, buscando um relacionamento cooperativo e satisfatório para ambas as partes, com objetivos comuns.

A ABNT NBR ISO/IEC 27002 (2013) aponta que, pessoas que desconhecem qualquer tipo de Política de Segurança da Informação, podem vazar dados sigilosos que consequentemente irão resultar na perda de credibilidade e confiabilidade da empresa no mercado.

Mitnick e Simon (2003, p. 04) afirmam que:

> A medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltarão cada vez mais para a exploração do elemento humano.

A segurança é responsabilidade de todos, se não há restrições, políticas e processos que definem e organizem a conduta do profissional dentro da corporação, as soluções tecnológicas mais sofisticadas, não tem sentido.

2.2. Segurança da Informação

Sêmola (2003) define Segurança da Informação como sendo uma área do conhecimento dedicada à proteção da informação contra acessos indevidos, alterações não autorizadas ou a sua indisponibilidade quando se faz necessário. No mesmo sentido a ABNT NBR ISO/IEC 27002 (2005, p. 10), destaca Segurança da Informação como " 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.".

A Segurança da Informação foi criada para proteger a informação no sentido de preservar o valor que possuem para um indivíduo ou uma organização. Cada tipo de informação deve ser examinado e classificado a partir de três princípios básicos, Sêmola (2003) os descreve da seguinte maneira:

- **Confidencialidade:** é a garantia do resguardo das informações dadas pessoalmente em confiança e a proteção contra a sua violação, somente pessoas devidamente autorizadas pela empresa devem ter acesso a essas informações.
- **Integridade:** as Informações devem ser manipuladas somente por pessoas previamente autorizadas e com a condição de manter todas as características originais estabelecidas pelo proprietário da informação. Dados não podem ser criados, alterados, ou removidos sem autorização, é a garantia de que a informação não será alterada durante a sua transmissão.
- **Disponibilidade:** a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado. Para que uma Informação demonstre disponibilidade, a organização deve dispor de um Sistema de Informação Computacional, com controles de segurança e canais de comunicação de bom funcionamento.

Para a ABNT NBR ISO/IEC 27002 (2013, p. 04), “a segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware”. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados e atualizados quando necessários, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos.

2.2.2. Ferramentas da Segurança da Informação

Fontes (2006) aborda que, desde o surgimento das primeiras ameaças, a Gestão de Segurança da Informação vem estabelecendo meios de se mensurar e proteger as informações de uma organização através do uso de ferramentas de proteção e prevenção, as mais importantes delas estão descritas nos subtópicos a seguir.

2.2.2.1. Antivírus

Os programas do tipo Antivírus **s**ão softwares que procuram detectar, anular e remover os vírus de computador e outros tipos de malware. Alguns tipos de Antivírus também inclui a funcionalidade de um Firewall (CERT.BR, 2012, p. 111), segue alguns exemplos abaixo:

- **Exemplos de Antivírus:** Avast Antivírus Free (versão gratuita) e Pro (versão paga), AVG Antivírus free e pro, Avira Antivírus free e pro, Kaspersky Antivírus pro, Norton Antivírus pro, etc.
- **Exemplos de Antivírus com Firewall:** Avast Internet Security, AVG Internet Security, Kaspersky Internet Security, Norton Internet Security, etc.

Para ajudar na escolha do Antivírus ideal, a empresa pode fazer uma pesquisa no site do laboratório AV Comparatives. Esta é uma organização independente que oferece testes sistemáticos verificando se o software de segurança, faz jus às suas referidas promessas.

2.2.2.2. Firewall

Conforme CERT.BR (2012, p. 57), Firewall é um software, mas também pode ser incorporado à um hardware. Sua função é controlar todo o tráfego de dados através da verificação das informações que entram e saem da rede a fim de garantir que não ocorram acessos indevidos.

Ainda de acordo com CERT.BR (2012, p. 57), quando bem configurado, o firewall pode ser capaz de:

- Registrar as tentativas de acesso aos serviços habilitados nos computadores;

- Bloquear o envio de informações para terceiros sem autorização;
- Bloquear as tentativas de invasão cometidas pelos hackers;
- Analisar continuamente o conteúdo das conexões, filtrando diversos tipos de código malicioso;
- Evitar que um malware já instalado seja capaz de se propagar, impedindo que afetem outros computadores na rede.

2.2.2.3. Certificação Digital

Seguindo a modernidade tecnológica, a assinatura (forma de comprovar a autenticidade de documentos) deixou de ser feita a mão e em papeis para ser digital e eletrônica. Assim ficou mais fácil a sua utilização, mas também aumentou a responsabilidade em mantê-la segura e inviolável. Para isso criou-se a Certificação Digital, que se trata de um tipo de tecnologia de identificação que permite que transações eletrônicas dos mais diversos tipos sejam realizadas considerando os aspectos da integridade, autenticidade e confidencialidade, de forma a evitar que adulterações, interceptações de informações privadas ou outros tipos de ações indevidas ocorram. (ALECRIM, 2016)

Desta maneira Alecrim (2016) descreve Certificado Digital como, um documento eletrônico com assinatura digital que possui validade jurídica, no qual garante proteção às transações eletrônicas e outros serviços via internet, permitindo que pessoas e empresas se identifiquem e assinem documentos digitalmente de qualquer lugar do mundo com mais segurança e agilidade. Com o certificado digital, a parte interessada obtém a certeza de estar se relacionando com a pessoa ou entidade esperada.

2.2.2.4. Criptografia

A Criptografia é mais uma das ferramentas de proteção a informação a serviço de todos. A proteção do envio e recebimento de mensagens sigilosas ou críticas sempre foram questões de necessidade e foi através da Criptografia que se conseguiu essa proteção extra de segurança.

CERT.BR (2012, p. 67) descreve Criptografia como, “ciência e arte de escrever mensagens em forma cifrada ou em código. ” Ela é um dos principais mecanismos de segurança que se pode utilizar para se proteger dos riscos associados aos envios de dados via Internet. CERT.BR (2012) ainda destaca que, a Criptografia utiliza dois tipos de chaves, a Simétrica e a Assimétrica:

- **Chave Simétrica**: é a mais comum das chaves de criptografia, ela se consiste na relação entre o emissor e o receptor, onde ambos possuem o mesmo tipo de chave, assim qualquer um dos dois pode enviar, quanto receber uma mensagem.
- **Chave Assimétrica**: esse modelo utiliza duas chaves distintas, uma chave pública (somente para codificar) e uma chave privada que a única capaz de traduzir a mensagem. Este método de Criptografia é considerado o mais seguro, tanto que sua principal utilização é feita pelos Bancos.

Ainda de acordo com CERT.BR (2012), a Criptografia pode ser usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancarias; proteger a integridade de transferências eletrônicas de fundos, e proteger o sigilo de comunicações pessoais e comerciais.

Através das afirmações acima podemos perceber como é processo de Criptografia de um documento, ao codificar (proteger com um código) uma informação a mesma só pode ser decodificada (desprotegida) por alguém que conhece o método e a chave da Criptografia utilizada, deixando assim as comunicações muito mais secretas. Logo abaixo, a figura 03 descreve melhor esse funcionamento:

Figura 03: Funcionamento da Criptografia.
Fonte: SANTANDER. Disponível em: <https://www.santander.com.br/portal/wps/script/templates/GCMRequest.do?page=6682>. Acesso em 12/07/2016.

2.2.2.5. Biometria

Brasil (2007) define o termo biometria como medição biológica, ou seja, é o estudo das características físicas e comportamentais de cada pessoa. Os sistemas biométricos são sistemas automáticos de verificação de identidade baseados em características físicas do

usuário. Esses sistemas têm como objetivo suprir deficiências de segurança das senhas, que podem ser reveladas ou descobertas.

Os sistemas biométricos são uma evolução natural dos sistemas manuais de reconhecimento usados há muito tempo, como a análise grafológica de assinaturas, a análise de impressões digitais e o reconhecimento de voz. Hoje já existem sistemas ainda mais sofisticados, como os sistemas de análise da conformação dos vasos sanguíneos na retina. A seguir estão os principais sistemas de leitura biométrica citados por Brasil (2007):

- **Impressão digital**: captação das linhas da impressão digital por meio de um leitor biométrico que impulsiona o sistema a compará-lo com seu banco de dados.
- **Reconhecimento facial**: realiza a leitura dos traços do rosto de um indivíduo.
- **Veias das mãos**: faz a captação de informações baseados nos volumes de veias aparentes das mãos de uma pessoa.
- **Identificação pela íris**: fotografia da íris do olho realizada sob uma iluminação infravermelha.
- **Identificação pela retina**: informações são coletadas por meio de um foco de luz.
- **Geometria da mão**: envolve a identificação do tamanho, da estrutura e da posição da palma da mão de uma pessoa.
- **Reconhecimento de voz**: analisa a sonoridade, a gravidade e os sinais agudos de uma voz.

2.2.2.6. Backup

O Backup é uma prática bastante utilizada por pessoas e empresas, garantindo uma ou mais cópias de segurança de documentos, imagens, vídeos e outros arquivos importantes. Monteiro (2007, p. 647) enfatiza melhor o seu significado:

> Backup é um termo inglês, consiste na obtenção de uma cópia de um arquivo em um meio de armazenamento separado do original, com o propósito de segurança de dados, de forma que se o arquivo original for apagado ou destruído acidentalmente tem-se a cópia alternativa (de backup) para utilização.

CERT.BR (2012) argumenta que, existem várias formas de se fazer um Backup, pode ser através de um computador, dispositivos móveis (HDs, pendrives, cartão de memória, CDs, etc.), e-mail e até mesmo nas “nuvens” (Sites hospedados na internet como, Dropbox, Google Drive, One Drive, Box, etc.).

Algumas formas de Backup são pagas, mas a importância de se ter uma cópia de segurança que permite restaurar seus dados perdidos quando necessário, não tem preço.

2.3. Políticas de Segurança da Informação (PSI)

As políticas de segurança quase sempre são construídas a partir das necessidades da empresa. As melhores práticas de proteção da informação devem ser incorporadas pelas organizações para assegurar o monitoramento contínuo dos dados e a sua integridade.

Fontes (2006) descreve que, a Política de Segurança da Informação (PSI) é um documento que deve conter um conjunto de normas, métodos e procedimentos, os quais devem ser comunicados a todos os funcionários, bem como analisado e revisado criticamente, em intervalos regulares ou quando mudanças se fizerem necessárias.

Ainda Fontes (2006) acrescenta que o SGSI que vai garantir a viabilidade e o uso dos ativos somente por pessoas autorizadas e que realmente necessitam delas para realizar suas funções dentro da empresa.

Contribuindo com Fontes (2006), Dantas (2011) pontua que, uma política de segurança é um documento que estabelece princípios, valores, compromissos, requisitos, orientações e responsabilidades sobre o que deve ser feito para alcançar um padrão desejável de proteção para as informações. Ela é basicamente um manual de procedimentos que descreve como as informações devem ser protegidas e utilizadas.

A partir das afirmações de Fontes (2006) e Dantas (2011), Sêmola (2003) assegura que esse conjunto de normas tem o propósito de definir regras, padrões e instrumentos de controle que deem uniformidade a um processo, produto ou serviço.

A norma ABNT NBR ISO/IEC 27002 (2013) entende que o objetivo principal de uma PSI é fornecer orientação e apoio a Gestão de Segurança da Informação de acordo com requisitos de negócio e as leis e regulamentos adequados.

“Atualmente, a PSI é adotada em grande parte das organizações em todo o mundo, inclusive no Brasil. Mesmo aquelas empresas que ainda não tem uma política efetiva, reconhecem a necessidade de elaborar e implementar uma”. (CAMPOS, 2007, p. 131).

Segundo a NBR ISO/IEC 27002 (2005), a PSI não precisa ser um documento a parte, ela pode ser uma parte de um documento da Política geral da empresa. Se a PSI for distribuída fora da organização, convém que sejam tomados todos os cuidados para não revelar informações sensíveis. É recomendado que a política de segurança da informação seja revisada periodicamente e de forma planejada ou quando ocorrerem mudanças significativas, para assegurar a sua continua pertinência, adequação e eficácia.

2.3.1. Norma ABNT NBR ISO/IEC 27002:2013

A ISO/IEC 27002:2013 é um guia de boas práticas em segurança da informação reconhecido internacionalmente, foi estruturada para fornecer a especificação de controles de segurança da informação dentro de uma organização, de acordo com os negócios da empresa.

O histórico apresentado pela ISO/IEC 27002 (2013) inicia em 1995 com o Departamento de Comércio e Indústria do Reino Unido (DTI), que através de seu Centro de Segurança de Informações (CCSC), criou uma norma de segurança das informações chamada "BS7799 (British Standard ou Padrão Britânico 7799) " para atender as organizações do País.

Em dezembro de 2000, após diversas alterações, a BS7799 ganhou status internacional com sua publicação na forma da ISO/IEC 17799:2000.

A Associação Brasileira de Normas Técnicas (ABNT) homologou em setembro de 2001 a versão brasileira da norma, denominada ABNT NBR ISO/IEC 17799.

A ABNT NBR ISO/IEC 17799 cobre os mais diversos tópicos da área de segurança, possuindo um grande número de controles e requerimentos que devem ser atendidos para garantir a segurança das informações de uma empresa. A partir de 2005, a nova edição da ABNT NBR ISO/IEC 17799 foi incorporada ao novo esquema de numeração como ABNT NBR ISO/IEC 27002:2005 que é um código de práticas para a Gestão Segurança da Informação.

Na Figura 04 é possível ver as alterações que a ABNT NBR ISO/IEC 27002:2013 sofreu em relação à anterior:

Seção	ISO/IEC 27002: 2005
5	Política de Segurança da Informação
6	Organizando a Segurança da Informação
7	Gerenciamento de Ativos
8	Segurança em Recursos Humanos
9	Segurança Física e do Ambiente
10	Gestão de Operações e Comunicações
11	Controle de Acesso
12	Aquisição, Desenvolvimento e Manutenção de SI
13	Gerenciamento de Incidentes de SI
14	Gerenciamento da Continuidade do Negócio
15	Conformidade

Seção	ISO/IEC 27002: 2013
5	Política de Segurança da Informação
6	Organizando a Segurança da Informação
7	Gerenciamento de Ativos
8	Segurança em Recursos Humanos
9	Controle de Acesso
10	Criptografia
11	Segurança Física e do Ambiente
12	Segurança das Operações
13	Comunicação de Segurança
14	Aquisição, Desenvolvimento e Manutenção de SI
15	Relacionamento com Fornecedor
16	Gerenciamento de Incidentes de SI
17	Aspectos da segurança da informação no BCM
18	Conformidade

Figura 04: Correções da norma ABNT NBR ISO/IEC 27002:2013 em relação a sua antecessora a ABNT NBR ISO/IEC 27002:2005.
Fonte: Antônio (2014).

A nova norma está dividida em 14 seções de controles de segurança da informação. Do capítulo um ao quatro a norma apresenta seu objetivo, termos e definições, apresenta como a norma está estruturada e fala sobre análise e tratamento de riscos. A partir do capitulo 5 ela começa a se referir diretamente as práticas de Segurança.

Se a corporação não possui uma norma de proteção de informações, a ISO 27002 pode fornecer as diretrizes para a criação de uma. A norma pode servir como um guia para a criação da postura de Segurança da empresa ou como uma boa diretriz de Segurança a ser usada pela organização. (NBR/IEC 27002, 2013).

2.3.2. Desenvolvimento de uma PSI

Para o desenvolvimento e elaboração de uma PSI, Ferreira e Araújo (2008) defendem o uso de um método criterioso e técnico, no qual possam ser sugeridas alterações na configuração de equipamentos, na escolha de tecnologias e definição de responsabilidades. Deve também expressar os objetivos dos tomadores de decisões quanto ao uso das informações.

As fases para o desenvolvimento de uma PSI de acordo com a normativa NBR ISO/IEC 27002 (2013), são:

Fase 01 - Levantamento de Informações: nesta fase são analisadas as informações sobre a empresa, afim de identificar quais os tipos de controles de segurança existentes, tais como:

- Obtenção de normas e padrões de segurança;
- Entendimento das necessidades da empresa;
- Analise dos procedimentos de segurança existente;
- Uso dos recursos da Tecnologia da Informação;
- Obter informações sobre os ambientes de negócio da organização.

Com base nas informações adquiridas é possível identificar a atual situação da segurança da organização e as suas necessidades.

Fase 02 - Desenvolvimento do conteúdo da Política de Segurança: aqui inicia-se o conteúdo da política, são definidas as regras e responsabilidades e como serão feitos os controles de segurança, como descrito abaixo:

- Objetivo da PSI;
- Classificação das Informações;
- Fatores críticos para a organização;

- Padrões e procedimentos;
- Gerenciamento e definição da PSI;
- Gerenciamento da versão e manutenção da política;
- Referência para outras políticas;
- Atribuições e responsabilidades.

Fase 03 - Elaboração dos procedimentos de Segurança da Informação: nesta fase é feito um estudo da concorrência, visando as ferramentas e práticas utilizadas pelo mercado e baseado nestas serão desenvolvidos os procedimentos para cada tipo de controle selecionado na fase anterior, tais como:

- Notificação e gerenciamento de incidentes;
- Processo disciplinar;
- Aquisição e uso de hardware e software;
- Proteção contra software malicioso;
- Uso correto da Internet;
- Utilização dos recursos de TI;
- Gerenciamento e controle da rede,
- Uso de Criptografia e gerenciamento de chaves;
- Controle de acesso às áreas sensíveis;
- Procedimentos de Backup.

Fase 04 - Revisão, aprovação e implantação da Política de Segurança: esta é a última fase da PSI, aqui os procedimentos criados anteriormente são revisados, a política é aprovada e implantada, e o seu conteúdo e regras são divulgados a todos os integrantes da empresa (de funcionários à gerencia) e as seguintes iniciativas serão tomadas:

- Atuação de todos os funcionários junto à área responsável pela PSI;
- Divulgação das responsabilidades dos colaboradores;
- Demonstração da importância das normas e procedimentos da PSI;
- Realização de palestras e treinamentos referentes a nova Políticas;
- Assinatura do termo de Sigilo, Confidencialidade e Responsabilidade.

Além destas quatro fases para a implantação de uma PSI, podemos citar mais uma que é tão importante quanto as outras, que é a fase de manutenção e atualização da mesma.

Segundo a própria NBR ISO/IEC 27002 (2013), o gerenciamento da PSI tem que estar em constante acompanhamento e sempre seguindo o mesmo ritmo da tecnologia, desta forma ela será sempre eficaz para a organização.

A ABNT NBR ISO/IEC 27002:2013 complementa que a manutenção periódica deve incluir avaliação de oportunidades para melhoria da organização da PSI e abordagem de Gestão de Segurança da Informação em resposta a mudanças no ambiente organizacional, circunstâncias de negócios, condições legais, ou ambiente técnico.

2.3.3. Características de uma PSI

De acordo com Fontes (2006), para uma Política de Segurança da Informação ser bem-sucedida, ela deverá possuir as seguintes características: linguagem simples; fácil compreensão e aplicação; clareza e concisão; estar de acordo com a realidade da empresa; realizar revisões periódicas; estar sempre atualizada.

Seguindo o mesmo princípio de Fontes (2006), Ferreira e Araújo (2008) afirma que para ser considerado uma Política de Segurança da Informação, a mesma deve conter as seguintes características:

SER VERDADEIRA	**SER COMPLEMENTADA COM A DISPONIBILIDADE DE RECURSOS**
Deve evidenciar o real pensamento da empresa e ser coerente com suas as ações.	Deve haver disponível recursos financeiros e de pessoal para que essa política possa ser implementada ao longo do tempo.
SER SIMPLES	**SER VÁLIDA PARA TODOS**
Deve ser de fácil leitura e compreensão.	Deve ser cumprida e respeitada por todos na empresa.
COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO DA ORGANIZAÇÃO	
Deve ser assinada pelo mais alto executivo, demonstrando assim, seu total apoio à política.	

Quadro 01: Características de uma Política de Segurança da Informação.
Fonte: Elaborado pelo autor, conforme Ferreira e Araújo (2008).

2.3.4. Certificação

Conforme descrito no Manual de Instruções do uso da Marca ABNT (ABNT PG-15.02, 2015), a certificação é um documento emitido por uma entidade certificadora independente, que garante que uma dada empresa implantou corretamente todos os controles

da norma aplicáveis. A certificação é emitida após um procedimento de verificação de conformidade da empresa pela entidade certificadora.

Com a certificação, a empresa certificada comprova que a segurança da informação está assegurada de forma efetiva, o que não significa, que a empresa esteja imune a violações de segurança. Além disso, a certificação comprova, para os clientes e fornecedores da empresa a importância que esta tem com a segurança de suas informações, melhorando a imagem da empresa no mercado.

A obtenção da certificação é um processo demorado e muito trabalhoso. De acordo com ABNT PG-15.02 (2015), o mesmo é dividido em três passos:

- O primeiro passo é a empresa adquirir o catálogo de normas (ABNT NBR ISO/IEC 27002:2013) para a implantação correta de uma PSI, esse catálogo está disponível para compra no site oficial da ABNT.
- Após a aquisição do documento o passo seguinte é implantar a política dentro da organização.
- E finalizando, o terceiro e último passo é solicitar a certificação junto à ABNT através do e-mail certificacao@abnt.org.br. A ABNT irá fiscalizar se está tudo dentro das conformidades exigidas e irá encaminhar todos os documentos necessários para o seu processo.

2.4. Gestão de Segurança da Informação

Em tempos remotos o setor de Tecnologia da Informação (TI) era o único responsável por tudo relacionado as Informações e as Tecnologias, mas com a grande revolução tecnológica e o uso constante de computadores, essa demanda ficou tão imensa que os Gestores (Diretores, Supervisores, Gerentes, Administradores, etc.) também passaram a contribuir na proteção de suas informações.

Nesse sentido, Laureano e Morais (2005, p. 06) pontua que “os administradores de hoje devem saber como estruturar e coordenar as diversas tecnologias de informação e aplicações de sistemas empresariais para atender às necessidades de informação de cada nível da organização e às necessidades da organização como um todo”.

Para Sêmola (2003), a gestão da segurança da informação pode ser classificada em três aspectos: tecnológicos; físicos e humanos.

- **Tecnológicos:** nesse aspecto incluem equipamentos e ameaças que se utiliza da tecnologia, tais como: redes; computadores; vírus; hackers; Internet; etc.

- **Físicos:** esse aspecto inclui toda a estrutura física da organização, como prédios, maquinas, instalações, etc.
- **Humanos:** como o próprio nome diz, são aspectos relacionados com as pessoas que fazem uso da Informação.

As organizações preocupam-se principalmente com os aspectos tecnológicos e se esquecem dos outros (físicos e humanos) tão importantes e relevantes para a segurança do negócio quanto os aspectos tecnológicos.

Netto e Silveira (2007, p. 381), "afirmam que a adequação de qualquer empresa à norma ISO IEC 27002:2005 garante conformidade com as melhores práticas em gestão da segurança da informação".

2.5. Relação das Informações Protegidas X A Imagem da Empresa

Qualquer pessoa que deposita algum tipo de informação em uma determinada companhia espera que esta esteja segura e disponível quando necessitar. E a empresa que gerencia o uso dessas informações deve se utilizar de diversas formas de proteção para a preservação deste patrimônio.

De acordo com Brunner (2012), a Informação é hoje o ativo mais importante para pessoas e empresas, alimentando todo o eixo que faz o mundo girar. E neste momento vivemos um contexto curioso, onde a informação é vasta, amplamente divulgada, acessível a quase todas as pessoas, e por muitas vezes banalizada, a ponto de tornar-se difícil a sua proteção.

Uma pesquisa realizada pela a EY Brasil (2013) em sua 16ª Pesquisa Anual Global sobre Segurança Cibernética, constatou-se um aumento na preocupação das empresas de como manter seus dados protegidos. Dos 1900 empresários entrevistados em 64 países, 31% deles relatam que a quantidade de incidentes relacionados a segurança em suas organizações aumentou pelo menos 5% nos últimos 12 meses. Muitos perceberam a relevância e a seriedade das ameaças imposta às empresas e como resultado disso, as questões relativas à segurança da informação contam com o apoio da alta administração em 70% das organizações pesquisadas.

3. MATERIAL E MÉTODOS

3.1 Perfil da empresa

A organização pesquisada é uma empresa do ramo da contabilidade que está situada no centro da cidade de Maracaju-MS, possui 13 (treze) funcionários e está a mais de 30 (trinta) anos no mercado e sempre se atualizando e acompanhando o crescimento do município.

O escritório contábil é considerado uma empresa familiar, pois desde sua fundação ela pertence à mesma família e a frente dos negócios estão dois sócios que tem como parentesco, mãe e filho. O filho formado em contabilidade, trabalha diretamente com os clientes e coordena os funcionários, já a mãe trabalha mais internamente na organização, sendo ela responsável pela verificação final em documentos, balanços patrimoniais, etc.

Em 2011 um dos Sócios Proprietários da empresa recebeu o prêmio “Mérito de Excelência na Gestão”, que é uma iniciativa da Federação dos Contabilistas, que tem como objetivo estimular a busca de conhecimento e agregar valor ao trabalho do profissional contábil.

A empresa está dividida em 4 (quatro) setores principais, o Gerencial, a Coordenação, o Setor Contábil (subdividido em Rural e Comercial) e o Financeiro/RH. Além desses temos uma recepção que faz atendimento a todos os setores. Logo abaixo é apresentado o organograma da empresa pesquisada com seus respectivos setores.

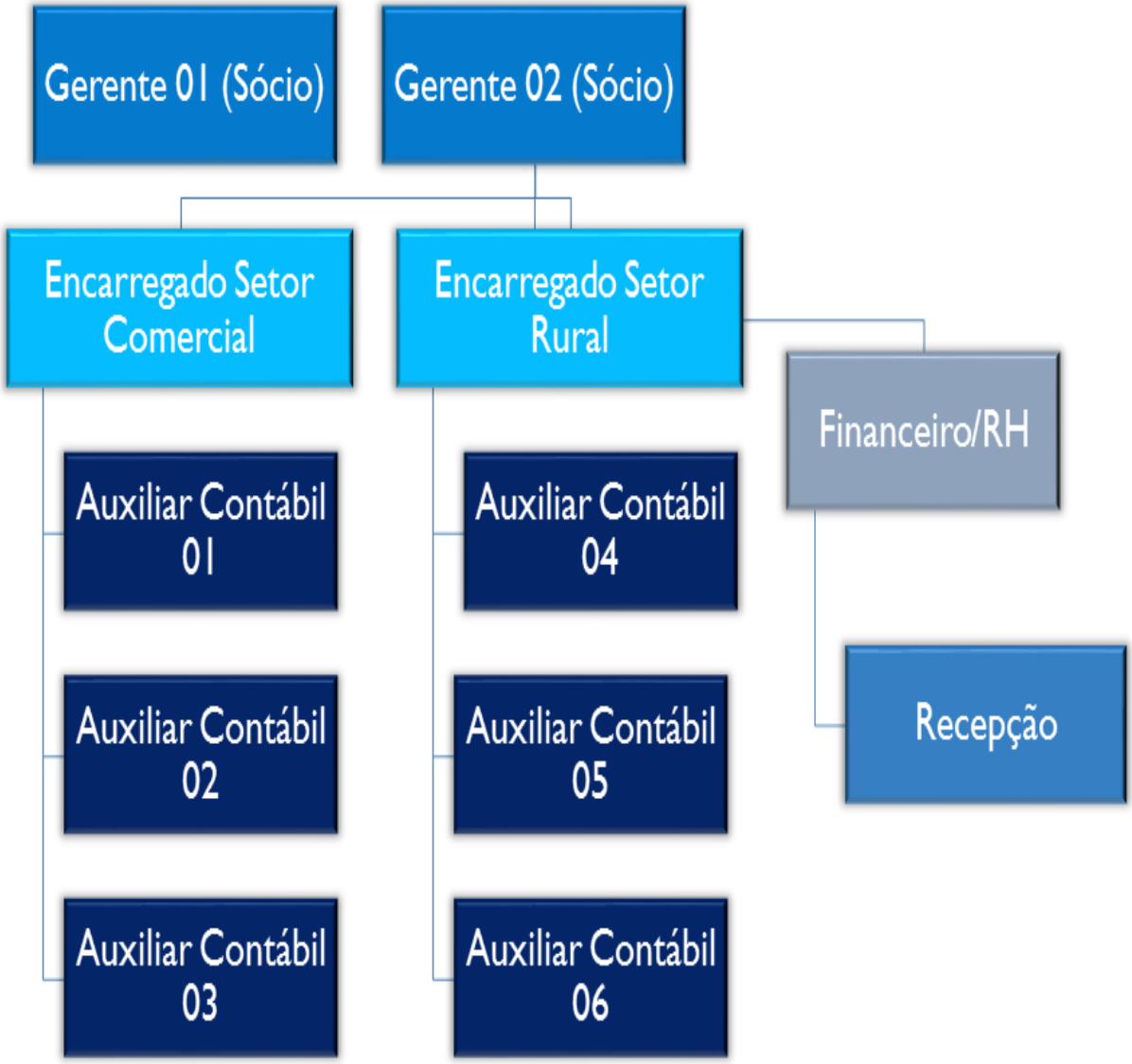

Figura 05 - Organograma da empresa pesquisada.

3.2 Cenário da Pesquisa

A metodologia aplicada se desenvolveu em duas fases: primeira foi feito o levantamento bibliográfico onde foram analisados livros e artigos científicos, além da norma ABNT ISO/IEC 27002:2013 para o embasamento teórico do trabalho. Para a pesquisa de campo, foram aplicados dois questionários estruturados com perguntas objetivas (questões fechadas), um dirigido a gerencia e o outro a 11 (onze) funcionários envolvidos diretamente na manipulação das informações, no período de 13 a 27 de agosto de 2016, com o objetivo de analisar a utilização de uma Política de Segurança da Informação na empresa.

Após isso, os dados foram resumidos em tabelas e tabulados utilizando os softwares IBM SPSS Statistics 22 e Microsoft Excel 2016.

4. RESULTADOS E DISCUSSÃO

4.1. Analise dos dados do questionário aplicado a gerencia

Observou-se que a empresa pesquisada é constituída por dois sócios proprietários, com idades acima de 30 anos, sendo um do sexo masculino graduado em Ciências Contábeis e outro do sexo feminino, com graduação em Administração e Ciências Contábeis e ambos atuam a mais de 5 (cinco) anos à frente da organização.

Para a análise das respostas dos gestores elaborou-se a seguir um quadro com o objetivo de evidenciar a relação existente entre as normas de Segurança da Informação com as práticas de segurança adotadas pela empresa.

Medidas de Segurança	Normas adotadas pela Empresa	Evidências Teóricas
Existência de Política de Segurança da Informação.	Existe uma norma interna de segurança na empresa, no entanto a mesma não é documentada.	A ABNT NBR ISO/IEC 27002 (2013) certifica que a direção da empresa precisa definir e aprovar um conjunto de Políticas de Segurança da Informação, publicar e comunicar a todos os funcionários e membros da organização.
Orientações referente ao funcionamento do Sistema de Segurança da empresa para os funcionários.	Os esclarecimento sobre as normas de segurança é feito verbalmente através de reuniões.	É necessário treinamento adequado que oriente os usuários para melhor utilização do Sistema de Segurança da empresa. Araújo e Ferreira (2008)
Orientações sobre a PSI da empresa para novos funcionários.	Assim que um novo funcionário é contratado, ele é informado sobre as normas de segurança da empresa.	A PSI da empresa deve ser publicada e comunicada a todos os funcionários e partes externas relevantes. ABNT NBR ISO/IEC 27002 (2013)
Recomendação referente ao uso de senhas diferentes para cada funcionário no ambiente de trabalho.	Todos os funcionários utilizam senhas diferentes.	É importante o uso de um loguin e senha de usuário único, para permitir relacionar os usuários com suas responsabilidades e ações. ABNT NBR ISO/IEC 27002 (2013)
Troca de senhas de segurança de ex-funcionário.	Quando um funcionário é desligado da empresa, suas senhas são alteradas.	Após o término do vínculo trabalhista, os direitos de acesso do funcionário devem ser removidos ou suspensos.

		ABNT NBR ISO/IEC 27002 (2013)
Acesso ao Servidor de dados.	O acesso ao Servidor é restrito à gerencia e o suporte técnico.	O acesso ao Servidor precisa ser restrito, de acordo com a política de controle de acesso. ABNT NBR ISO/IEC 27002 (2013)
Existência de Backup.	O backup de todo o Sistema de Informação da empresa é feito periodicamente.	De acordo com ABNT NBR ISO/IEC 27002 (2013), os backups são cópias de segurança que devem ser feitas e testadas regularmente.
Há Nobreak ou geradores de energia.	Todos os computadores são equipados com Nobreaks.	"Convém que os equipamentos sejam protegidos contra falta de energia elétrica". (ABNT NBR ISO/IEC 27002, 2013, p.51)
Uso de software de proteção.	Todos os computadores possuem programa antivírus.	Para a segurança das Informações é obrigatório o uso de software antivírus em todos os computadores, principalmente no servidor. Araújo e Ferreira (2008)
Restrição à acessos na Internet.	O acesso à internet passa a ser restrito quando a mesma é utilizada sem relação ao trabalho.	É de extrema importância o gerenciamento de direitos de acesso em um ambiente distribuído e conectado à rede de internet. ABNT NBR ISO/IEC 27002 (2013)
Vistoria periódica de equipamentos.	Mensalmente são feitas vistorias nos equipamentos, através de empresas de suporte terceirizada.	"Convém que os equipamentos tenham uma manutenção correta para assegurar sua disponibilidade e integridade permanente". (ABNT NBR ISO/IEC 27002, 2013, p.52)
Informação como ativo principal da empresa.	A empresa considera a Informação como seu principal ativo.	A informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional e saúde da empresa. Sêmola (2003)

Quadro 02 - Relação existente entre as normas de Segurança da Informação com as práticas de segurança adotadas pela empresa.

Constatou-se no Quadro 02, que os gestores possuem algum entendimento sobre Segurança da Informação e procuram colocar em prática, com adoção de software antivírus em todos os computadores, sistema de backup, proteção quanto à queda de energia, atualizações de equipamentos, suporte técnico terceirizado especializado, restrições de acesso as informações, etc.

Podemos observar também a preocupação da empresa em retirar todo o acesso de antigos funcionários e exigir que cada colaborador faça uso de senhas diferentes. Desta maneira cada funcionário é responsável pelos seus próprios atos.

Outro ponto importante é que a empresa tenta transmitir aos novos funcionários e aos antigos, conhecimentos, a respeito de seu Sistema de Informação e as suas regras de segurança. Porem a norma interna de segurança adotada pela empresa é somente transmitida aos funcionários de forma verbal, devido a mesma não ser documentada, isso dificulta sua aplicação prática e distancia a organização de possuir uma certificação ISO.

4.2. Analise dos dados do questionário aplicado aos funcionários

Para análise e discussão dos resultados adotou-se a seguinte estrutura: os dados socioeconômicos (idade, sexo, escolaridade e função), são apenas comentados devido a não terem relação direta com o assunto aqui pesquisado (Política de Segurança da Informação). Já os resultados que possuem relação direta são analisados e discutidos juntamente com os seus devidos gráficos, para que assim, possamos ter um melhor entendimento do estudo em questão.

Idade	**Frequência**	**Porcentagem**
De 18 a 25 anos	2	18,2
De 26 a 30 anos	3	27,3
De 31 a 40 anos	6	54,5
Total	**11**	**100,0**

Tabela 01 – Idade dos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016.

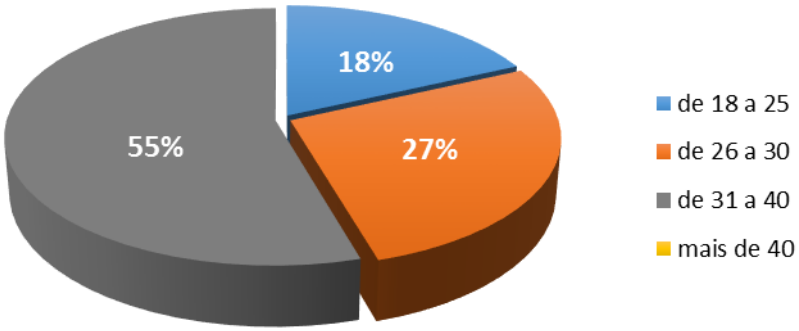

Gráfico 01 - Idade dos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016.

Através dos gráficos 01 ao 02, constatou-se que 55% dos funcionários tem entre 31 a 40 anos, 27% 26 a 30 anos e apenas 18% estão entre 18 a 25 anos.

Sexo	**Frequência**	**Porcentagem**
Masculino	1	9,1
Feminino	10	90,9
Total	**11**	**100,0**

Tabela 02 - Sexo dos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016.

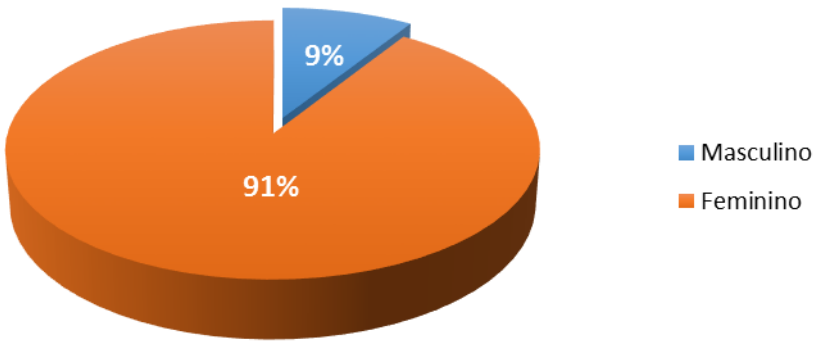

Gráfico 02 - Sexo dos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016.

Em relação ao sexo, 91% dos funcionários são do sexo feminino e apenas 09% do sexo masculino, isso nos mostra uma predominância muito grande do público feminino.

Escolaridade	**Frequência**	**Porcentagem**
Médio completo	1	9,1
Superior incompleto	8	72,7
Superior Completo	2	18,2
Total	**11**	**100,0**

Tabela 03 - Escolaridade dos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016.

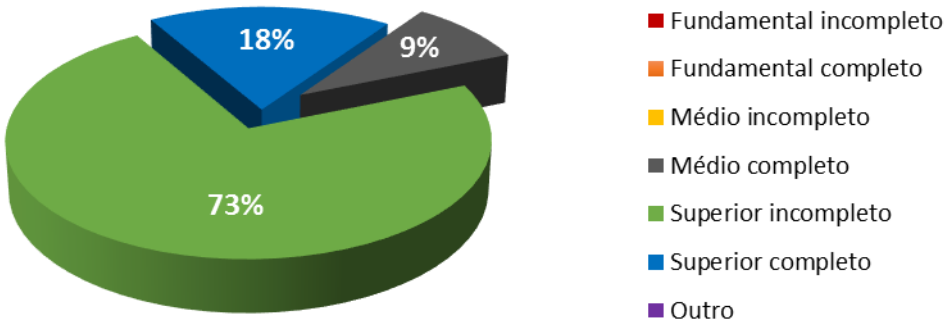

Gráfico 03 - Escolaridade dos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016.

A respeito do grau de escolaridade, podemos observar de acordo com o gráfico 03, que a maioria dos funcionários pesquisados (73%) possui Ensino Superior Incompleto, 18% já são formados e apenas 9% ou 1 (um) funcionário tem somente Ensino Médio Completo. Isso nos leva a crer que em geral os pesquisados têm um grau de instrução que lhes permitem compreender melhor as regras e normas da organização. E que a maioria está buscando se especializar através de uma faculdade, ou pelo menos tentaram melhorar seus conhecimentos.

Cargo/função ocupada	Frequência	Porcentagem
Office Girl	1	9,1
Recepcionista	1	9,1
Auxiliar de RH/Contábil/Financeiro	7	63,6
Encarregado	2	18,2
Total	**11**	**100,0**

Tabela 04 – Cargo/função ocupado pelos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016.

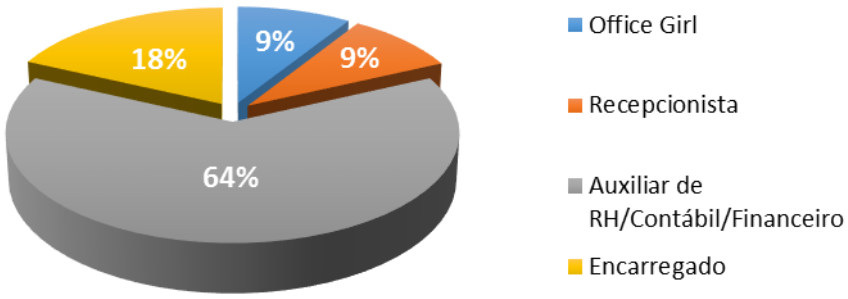

Gráfico 04 – Cargo/função ocupado pelos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016.

Com relação ao cargo/função que cada funcionário ocupa na empresa, o gráfico 04 mostra que 64% trabalha como auxiliar nos setores Contábil, Financeiro e Recursos Humanos. Representando 18 % temos dois encarregados, sendo um deles responsável pelos serviços contábeis rural e o outro comercial. E com apenas 9 % temos uma office girl (responsável pelo transporte e documentes entre a empresa e clientes). Além desses cargos o escritório também conta com uma recepcionista, que presta serviços para ambos os setores.

Tempo de empresa	Frequência	Porcentagem
Menos de 1 ano	1	9,1
Entre 1 a 2 anos	4	36,4
Mais de 5 anos	6	54,5
Total	**11**	**100,0**

Tabela 05 - Tempo de vínculo trabalhista dos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016.

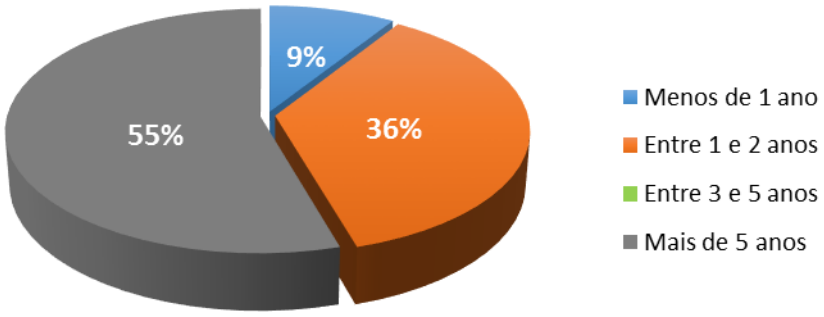

Gráfico 05 – Tempo de vínculo trabalhista dos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016.

A respeito do tempo do vínculo que cada funcionário possui com a empresa, foi constatado que, mais da metade, ou seja, 55% trabalham na organização a mais de 5 (cinco) anos, o que nos mostra que devem possuírem um bom conhecimento sobre a empresa e suas atividades. Os outros 36% estão na empresa entre 1 e 2 anos, e também nos leva a crer que possuem um pouco de bagagem e somente com 9% ou um funcionário, está na empresa a menos de 1 (um) ano.

Podemos observar que a maioria dos funcionários trabalham a bastante tempo na empresa e esse convívio de longa data permite que conheçam melhor o seu local de trabalho, como também é mais fácil de se praticar regras e normas, quando se está a par dos negócios da organização.

Sabe o que é PSI	Frequência	Porcentagem
Sim	11	100,0
Total	**11**	**100,0**

Tabela 06 - Conhecimento sobre Política de Segurança da Informação dos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016.

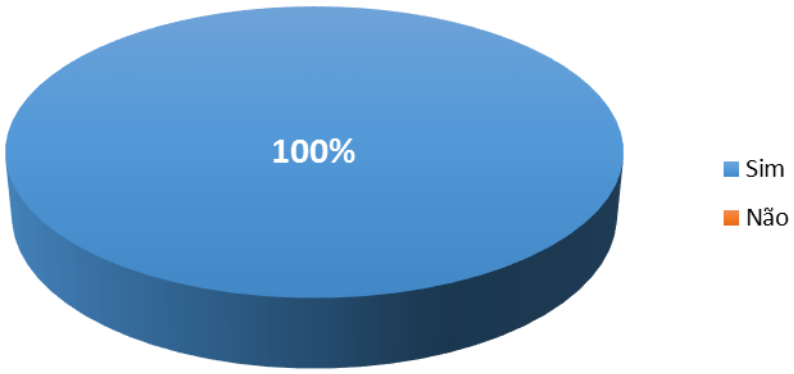

Gráfico 06 – Conhecimento sobre Políticas de Segurança da Informação dos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016.

Ao serem questionados se sabem o que é uma Política de Segurança da Informação (PSI), foram unanimes ao responderem que sim.

É essencial para manter protegido os ativos de informação, que cada funcionário saiba o real significado de uma Política de Segurança da Informação e a sua importância para a organização.

A ABNT NBR ISO/IEC 27002 (2013) aponta que, pessoas que desconhecem o significado de uma Política de Segurança da Informação, podem vazar dados sigilosos que consequentemente irão resultar na perda de credibilidade e confiabilidade da empresa no mercado.

Partindo desse mesmo princípio, Dantas (2011) explica que uma política de segurança é basicamente um manual de procedimentos que descreve como as informações devem ser protegidas e utilizadas, mas para que isso aconteça todos devem compreender o seu significado.

Conhece a PSI da empresa	Frequência	Porcentagem
Sim	8	72,7
Não	3	27,3
Total	**11**	**100,0**

Tabela 07 - Conhecimento dos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016 sobre a PSI utilizada na empresa.

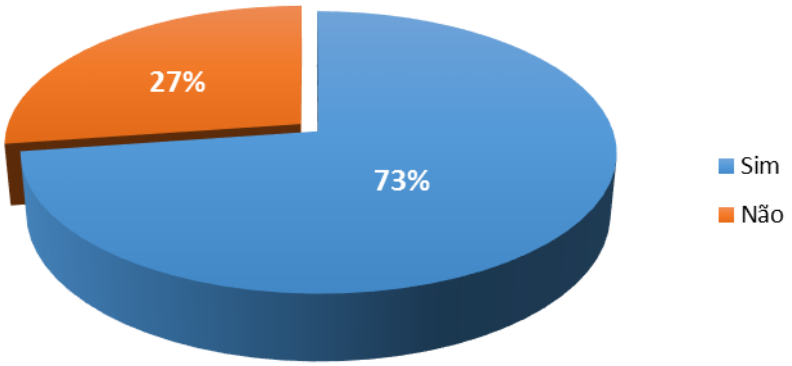

Gráfico 07 – Conhecimento dos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016 sobre a PSI utilizada na empresa.

A respeito de possuírem conhecimento da Política de Segurança da Informação utilizada na empresa, 73% responderem que sim e 27% desconhece totalmente a PSI da organização.

Podemos observar que a maioria dos entrevistados dizem ter conhecimento da PSI da empresa, mas o grande problema é os 27% que não conhecem. Conhecer a Política de Segurança da Informação da empresa é sem dúvida o ponto de partida para o manuseio correto e a proteção das informações.

Para a ABNT ISO/IEC 27002 (2013) é preciso que as Políticas de Segurança da Informação sejam comunicadas a todos os funcionários de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes.

Resposta similar foi obtida na pesquisa de Nascimento (2014), onde 57% dos funcionários tinha total conhecimento das práticas e normas de segurança da empresa.

Forma que Recebem Orientações	Frequência	Porcentagem
Através de reuniões	6	54,5
Através de treinamentos e reuniões	2	18,2
Não recebem orientações	3	27,3
Total	**11**	**100,0**

Tabela 08 - A forma que os participantes da pesquisa, escritório contábil, Maracaju-MS, 2016 recebem orientações sobre o Sistema de Segurança da Informação da empresa.

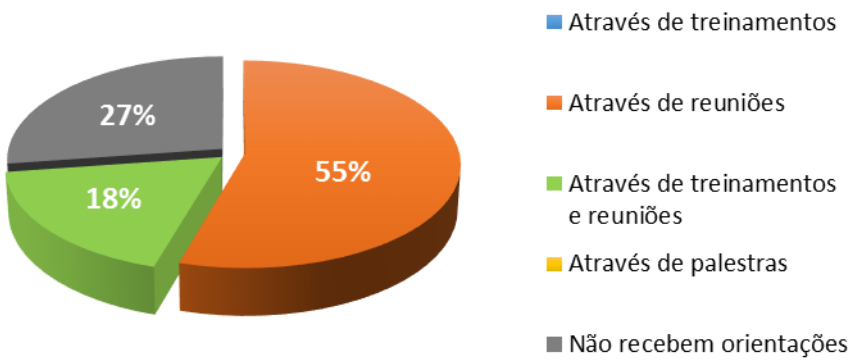

Gráfico 08 – A forma que os participantes da pesquisa, escritório contábil, Maracaju-MS, 2016 recebem orientações sobre o Sistema de Segurança da Informação da empresa.

Sobre receberem orientações a respeito do Sistema de Segurança da Informação da empresa e de que forma essas informações são passadas, 62% afirmam receber orientações através de reuniões, 15% através de treinamentos e 23% disseram que não recebem orientações sobre esse assunto.

Para um bom relacionamento interpessoal e um trabalho bem feito, o funcionário tem que estar a par do que acontece na empresa (regras, normas, procedimentos, etc.), principalmente quando se trata de segurança. Para isso a empresa tem que oferecer maneiras de orientar e qualificar esse profissional, como dito logo abaixo pela NBR ISO/IEC 27002 (2013)

> "Um sistema de gestão da segurança da informação bem sucedido requer apoio de todos os funcionários da organização. Isto pode também exigir a participação de acionistas, fornecedores ou outras partes externas. Orientações de especialistas externos podem também ser necessárias". (NBR ISO/IEC 27002, 2013, p. 04)

Nascimento (2014), também observou que, 59% dos funcionários não recebiam treinamento e nem orientações com relação ao Sistema de Segurança da organização e os demais receberam treinamento apenas com relação ao Sistema Contábil utilizado pelo escritório.

Restrição de Acesso	**Frequência**	**Porcentagem**
Sim	10	90,9
Não	1	9,1
Total	**11**	**100,0**

Tabela 09 – Há restrição de acesso as informações no escritório contábil, Maracaju-MS, 2016.

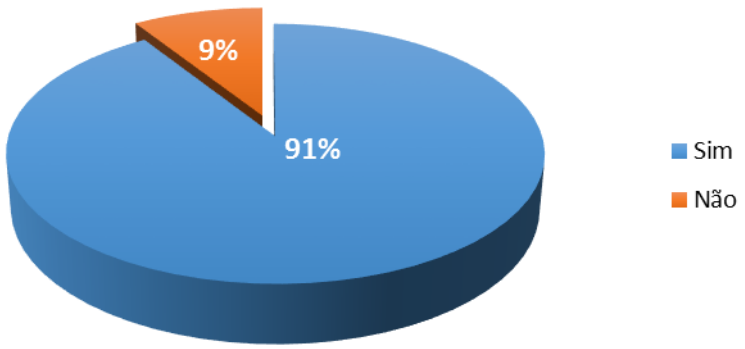

Gráfico 09 – Há restrição de acesso as informações no escritório contábil, Maracaju-MS, 2016.

Quando questionados sobre a existência de restrições de acesso as informações no âmbito da empresa, a maioria, 99% disseram que sim e que o acesso total é somente para a gerencia. Entretanto confrontando a resposta dos demais, 9% ou 1 (um) funcionário disse não haver esse tipo de restrição.

Toda empresa deve ter seu controle de acesso as informações de acordo com o seu grau de importância, e isso além de proteger as informações, também impede que segredos críticos da organização sejam revelados.

A ABNT NBR ISO/IEC 27002 (2013) afirma que o acesso à informação e às funções dos sistemas de aplicações devem ser restritos, de acordo com os requisitos das aplicações individuais do negócio e de acordo com a política de controle de acesso definida.

Ainda de acordo com a ABNT NBR ISO/IEC 27002 (2013), é preciso que as empresas determinem regras apropriadas do controle de acesso, direitos de acesso e restrições para papéis específicos dos usuários acessarem seus ativos, com o nível de detalhe e o rigor dos controles que reflitam os riscos de segurança da informação associados.

Dois princípios são importantes para orientar a política de controle de acesso, são eles: **a necessidade de conhecer:** você somente tem permissão para acessar informação que você necessita para desempenhar suas tarefas; **a necessidade de uso:** você somente tem permissão para acessar os recursos de processamento da informação (equipamentos de TI, aplicações, procedimentos, salas), que você necessita para desempenhar a sua tarefa/função/papel. (ABNT NBR ISO/IEC 27002, 2013)

Nascimento (2014) chegou em um resultado semelhante, porém com um percentual mais preocupante, onde 65% dos funcionários disseram que havia uma hierarquia de acesso à informação nos escritórios, mas 35% desconhecem essa restrição.

Descarte Físico	**Frequência**	**Porcentagem**
Sim	2	18,2
Não	9	81,8
Total	**11**	**100,0**

Tabela 10 - Descarte de um dado/informação fisicamente pelos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016.

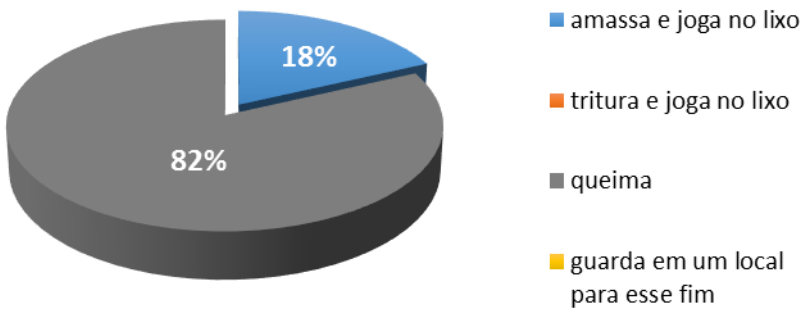

Gráfico 10 – Descarte de um dado/informação fisicamente pelos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016.

A respeito da forma que é descartado fisicamente um dado/informação quando o mesmo deixa de ser útil para a empresa, 82% disseram que queimam e 18% simplesmente amassa e joga no lixo. Quando um dado/informação não tem mais serventia para a empresa, ele tem que ser descartado de maneira que ninguém possa a vir recuperar. Para isso existem duas formas corretas, a ABNT ISO/IEC 27002 (2013) sugere que, uma mídia física contendo informações que não forem mais necessárias, devem ser destruídas de forma segura e protegida, através de incineração ou trituração.

Netto e Silveira (2007) chegaram a um resultado totalmente oposto a esse. Em sua pesquisa foi constatado que 87% dos funcionários não fazia o descarte correto das informações e o destino final era o lixo.

Descarte Lógico	**Frequência**	**Porcentagem**
Sim	10	90,9
Não	1	9,1
Total	**11**	**100,0**

Tabela 11 - Descarte de um dado/informação logicamente pelos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016.

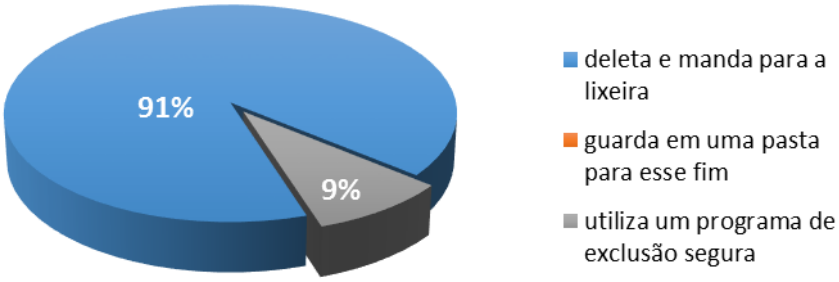

Gráfico 11 – Descarte de um dado/informação logicamente pelos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016.

Quanto a maneira que um dado/informação (quando não é mais útil para a empresa) é descartado logicamente, 91% deleta e manda para a lixeira e apenas 9% ou 1 (um) funcionário utiliza um software de exclusão segura.

Não é preciso ser um gênio em informática para recuperar um dado/informação da lixeira e mesmo excluindo da lixeira ainda é possível a sua recuperação, por isso é importante que se use um software específico para esse fim, como recomendado logo abaixo pela ABNT ISO/IEC 27002 (2013).

A ABNT ISO/IEC 27002 (2013), sugere que os procedimentos para o descarte lógico e seguro das informações devem ser através de software de remoção irreversível. E se houver informações importante em equipamentos danificados, a empresa deve fazer uma avaliação de riscos para determinar se vale a pena conserta-los para recuperar essas informações ou se é melhor que os itens sejam destruídos para que não haja vazamento de dados.

É preocupante saber que 91% dos funcionários dá fim a uma informação simplesmente mandando para a lixeira, isso comprova a teoria de Araújo e Ferreira (2008) quando dizem que os usuários têm que receber treinamentos adequados para que possa melhorar a utilização de ferramentas que garantam a proteção da informação em todas as partes de seu ciclo, inclusive no descarte.

Conhece seu Computador	Frequência	Porcentagem
Sim	7	63,6
Não	4	36,4
Total	**11**	**100,0**

Tabela 12 - Conhecimento sobre seu computador e seus principais programas dos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016.

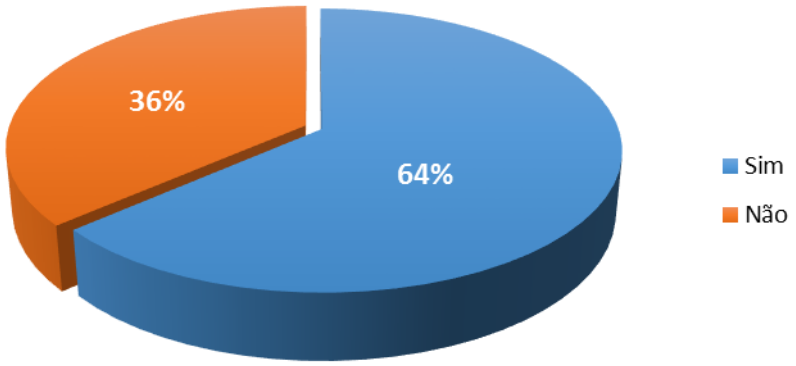

Gráfico 12 – Conhecimento sobre seu computador e seus principais programas dos participantes da pesquisa, escritório contábil, Maracaju-MS, 2016.

Ao serem questionados se tinham total conhecimento sobre seu computador e seus principais programas, 64% afirmaram que sim. Mas 36% disseram não conhecer direito o próprio instrumento de trabalho.

Conhecer a sua ferramenta de trabalho é o mínimo que se espera de um profissional, além de evitar acontecimentos negativos, agiliza e facilita o trabalho.

É responsabilidade dos gestores assegurarem que os funcionários tenham as habilidades e qualificações apropriadas sobre seu equipamento de trabalho e que sejam treinados antes de exercerem suas respectivas funções. (NBR ISO/IEC 27002, 2013)

De acordo com Laureano e Moraes (2005) a falta de conhecimentos na operação de equipamentos é uma das causas de vulnerabilidade em qualquer empresa. Segundo os autores, o início de um Sistema de Informação seguro, começa no reconhecimento de cada setor de trabalho.

Possui Nobreak	Frequência	Porcentagem
Sim	11	100,0
Total	**11**	**100,0**

Tabela 13 - Existência de Nobreak nos computadores no escritório contábil, Maracaju-MS, 2016.

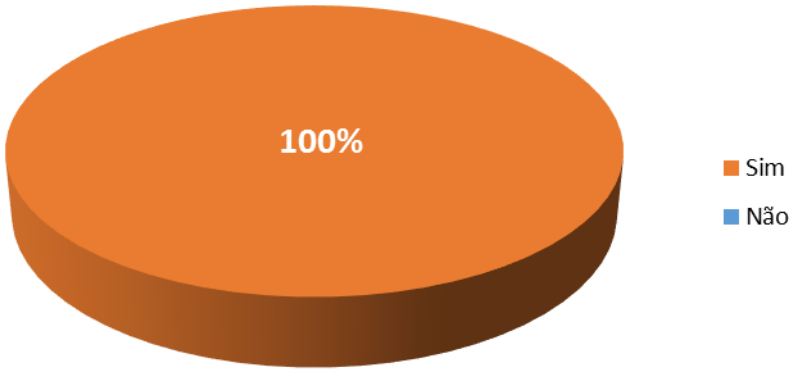

Gráfico 13 – Existência de Nobreak nos computadores no escritório contábil, Maracaju-MS, 2016.

Quanto aos computadores da empresa possuírem Nobreak como forma de segurança quanto a queda de energia, todos os funcionários confirmaram a existência do equipamento.

A utilização de Nobreak ou geradores de energia é muito importante para empresa, pois quando falta energia elétrica você consegue salvar todos os seus trabalhos e desligar seu computador sem que haja perda de dados.

Segundo a ABNT NBR ISO/IEC 27002 (2013), é preciso que os equipamentos sejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades e que seja providenciada antecipadamente, iluminação e comunicação de emergência.

Em sua pesquisa Netto e Silveira (2007) verificaram que pouco mais de 50% dos computadores da empresa pesquisada possuía equipamentos contra falhas de energia, fato que julgaram interessante, pois o Nobreak não é uma ferramenta de difícil implementação, requer baixo investimento e a percepção da gerência sobre sua importância.

5. CONSIDERAÇÕES FINAIS

O referido estudo demonstrou por parte da gerencia, que os gestores possuem algum entendimento sobre Segurança da Informação e que também já havia uma Norma Interna de Segurança na empresa, mas que precisa ser melhorada e documentada para ser considerada uma Política de Segurança da Informação. Por parte dos funcionários, todos dizem ter conhecimento do que é uma Política de Segurança da Informação, mas somente parte deles conhecem as Normas de Segurança da empresa.

No desenvolver deste trabalho, notou-se que as principais ações de segurança adotadas pela organização para preservar suas informações são: o antivírus instalado em todos os computadores, restrições de acesso, políticas de senhas, proteção quanto a queda de energia, backup e a manutenção periódica dos equipamentos por empresas terceirizadas. Segundo os gestores, a empresa considera a Informação como sendo seu principal ativo e além das Normas de Segurança adotadas, ela ainda orienta os funcionários através de reuniões.

De acordo com os entrevistados, esse modelo de proteção a Informação adotado pela empresa está sendo eficiente, porém não está de acordo com a norma ISO/IEC 27002:2013. Por não se tratar de uma norma documentada, dificultando o acesso e o conhecimento de todos. Em contrapartida a gerencia já manifestou interesse em criar uma PSI legalmente documentada e pretende contar com a ajuda de todos os envolvidos para colocá-la em prática e com isso obter uma certificação ISO padronizada.

Enfim, acredita-se que o trabalho atingiu seu propósito, uma vez que, gerencia e colaboradores da organização pesquisada, compreenderam a importância de se ter uma Política de Segurança documentada e de fácil acesso, visto que proteger seu principal ativo é responsabilidade de todos.

REFERÊNCIAS

AGRASSO, M. N.; ABREL, A. F. **Tecnologia da Informação: manual de sobrevivência da nova empresa.** São Paulo: Arte e Ciência, 2000.

ALECRIM, E. InfoWester. **O que é Certificação Digital?** Publicado em: 21/03/2016. Disponível em: <http://www.infowester.com/assincertdigital.php>. Acesso em: 18/07/2016.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002**. Técnicas de segurança - Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002**. Técnicas de segurança - Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT PG-15.02**. Manual de Instruções do uso da Marca ABNT. Rio de Janeiro, 2015.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. 2 ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2007.

BRUNNER, M. EZ Security. **O ativo mais importante – a Informação.** Disponível em: <http://www.ez-security.com.br/index.php/noticias/70-o-ativo-mais-importante-a-informacao>. Acesso em: 25/09/2015.

CAMPOS, A. **Sistemas De Segurança Da Informação**. 2. ed. Florianópolis: Visual Books, 2007.

CERT-BR. **Cartilha de Segurança para Internet**. Versão 4.0. São Paulo: Comitê Gestor da Internet no Brasil, 2012.

DANTAS, M. L. **Segurança da informação: uma abordagem focada em gestão de riscos.** Olinda: Livro Rápido, 2011.

EY BRASIL. **Crimes cibernéticos são a maior ameaça à sobrevivência das empresas.** Disponível em: <http://www.ey.com/BR/pt/Services/Release_Pesquisa_Seguranca_Informacao_EY>. Acesso em: 28/09/2015.

FERREIRA, F. N. F.; ARAÚJO, T. **Política de Segurança da Informação – Guia Prático para Elaboração e Implementação**. 2. ed. Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

FILHO, A. M. S**. Segurança da Informação: Sobre a Necessidade de Proteção de Sistemas de Informações**. In: Revista Espaço Acadêmico Ano IV. Nº 12. Novembro, 2014 - Mensal. ISSN 1519-6186.

FONTES, E. L. G. **Segurança da Informação: o usuário faz a diferença**. 1 ed. São Paulo: Saraiva, 2006.

HOUAISS, A.; VILLAR, M. S. **Dicionário Houaiss da Língua Portuguesa**. 3. ed. Rio de Janeiro: Objetiva, 2009.

LAUREANO, M. A. P.; MORAES, P. E. S. **Segurança como estratégia de gestão da informação**. Revista Economia e Tecnologia - ISSN 1415-451X, v. 8, fascículo 3, p. 38-44, 2005.

MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar - Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação**. São Paulo: Pearson, 2003.

MONTEIRO, M. A. **Introdução a Organização de Computadores**. 5. ed. Rio de Janeiro: LTC, 2007.

NASCIMENTO, T. R. L. **Segurança da Informação**: sua utilização pelos profissionais de escritórios contábeis em Pimenta Bueno – RO. Cacoal: Ed. UNIR, 2014.

NASCIMENTO, T. R. L. **Segurança da Informação**: sua utilização pelos profissionais de escritórios contábeis em Pimenta Bueno – RO. Cacoal: Ed. UNIR, 2014 apud LAUDON, Kenneth C.; LAUDON, Jane Price. **Sistemas de Informação: com Internet**. 4. ed. Rio de Janeiro: LTC,1999.

NETO, A. S.; SILVEIRA, M. A. P. **GESTÃO DA SEGURANÇA DA INFORMAÇÃO: Fatores que Influenciam sua Adoção em Pequenas e Médias Empresas.** Revista de Gestão da Tecnologia e Sistemas de Informação. Vol. 4, No. 3. São Caetano do Sul: IMES, 2007.

REZENDE, D. A.; ABREU, A. F. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais**. São Paulo: Atlas, 2000.

SÊMOLA, M. **Gestão da Segurança da Informação – Uma visão Executiva.** Rio de Janeiro: Elsevier, 2003.

TURBAN, E.; et. al. **Tecnologia da Informação para a Gestão: Transformando os Negócios na Economia Digital.** 6. ed. Porto Alegre: Bookman, 2010.

APÊNDICE

Apêndice A - Modelos dos questionários aplicados no estudo de caso

O modelo de questionário apresentado a seguir constitui, na íntegra, o instrumento de coleta de dados aplicado junto aos sujeitos de pesquisa (respondentes). Questionário anexado a seguir, utilizando-se as próximas 04 (quatros) páginas.

Questionário Operacional

As informações referentes a este questionário são unicamente para a realização de um TRABALHO DE PESQUISA exigido pela UNIVERSIDADE ESTADUAL DE MATO GROSSO DO SUL (UEMS). Com o objetivo de mostrar a importância da utilização de uma política de segurança da informação.

1. Qual a sua idade?
( ) de 18 a 25 ( ) de 31 a 40
( ) de 26 a 30 ( ) mais de 40

2. Sexo: ( ) Masculino
( ) Feminino

3. Escolaridade:
( ) Ensino fundamental incompleto ( ) Superior incompleto
( ) Ensino fundamental completo ( ) Superior completo
( ) Ensino médio incompleto ( ) Nível técnico
( ) Ensino médio completo ( ) Outro _____

4. Qual cargo você ocupa na empresa? _____
5. Há quanto tempo é funcionário dessa empresa?
( ) menos de 1 anos ( ) entre 3 e 5 anos
( ) entre 1 e 2 anos ( ) mais de 5 anos

6. Você sabe o que é uma Política de Segurança da Informação?
( ) Sim
( ) Não

7. Você conhece a Política de Segurança da Informação utilizada pela empresa?
( ) Sim
( ) Não

8. Você recebe orientações sobre o que é e como funciona o Sistema de Segurança da Informação da empresa? Se sim, de que forma?
( ) Sim, através de:
( ) treinamentos ( ) palestras
( ) reuniões ( ) outros
( ) Não

9. Você tem acesso a qualquer informação dentro da empresa?
( ) Sim
( ) Não

10. Como você descarta ou apaga, um dado/informação fisicamente?
( ) amassa e joga no lixo ( ) queima
( ) tritura e joga no lixo ( ) guarda em um local para esse fim

11. Como você descarta ou apaga, um dado/informação logicamente?
( ) deleta e manda para lixeira ( ) guarda em uma pasta para esse fim
( ) utiliza um programa de exclusão segura

12. Você conhece bem o seu computador e seus principais programas?
( ) Sim
( ) Não

13. No seu computador há nobreak ou geradores de energia, que garantam o suprimento de força quando há falta de abastecimento de energia?
( ) Sim
( ) Não

Questionário Gerencial

As informações referentes a este questionário são unicamente para a realização de um TRABALHO DE PESQUISA exigido pela UNIVERSIDADE ESTADUAL DE MATO GROSSO DO SUL (UEMS). Com o objetivo mostrar a importância da utilização de uma política de segurança da informação.

1. Qual a sua idade?
( ) de 18 a 25 ( ) de 31 a 40
( ) de 26 a 30 ( ) mais de 40

2. Sexo: ( ) Masculino
( ) Feminino

3. Escolaridade:
( ) Ensino fundamental incompleto ( ) Superior incompleto
( ) Ensino fundamental completo ( ) Superior completo
( ) Ensino médio incompleto ( ) Nível técnico
( ) Ensino médio completo ( ) Outro _____

4. Qual cargo você ocupa na empresa? _____

5. Há quanto tempo está na empresa?
( ) menos de 1 anos ( ) entre 3 e 5 anos
( ) entre 1 e 2 anos ( ) mais de 5 anos

6. Quantos funcionários a empresa possui? _____

7. Quantos funcionários estão envolvidos diretamente na manipulação das informações?
_____

8. Ao contratar um novo funcionário lhe são passadas as responsabilidades referentes à segurança da informação utilizada pela empresa?
( ) Sim
( ) Não

09. É recomendado aos usuários, usar senhas diferentes, ou todos utilizam a mesma senha no ambiente de trabalho?
( ) Sim, eles usam senha diferentes.
( ) Não, todos usam a mesma senha.

10. Quando um funcionário deixa de trabalhar na empresa, as senhas do local de trabalho utilizado por ele são trocadas?
( ) Sim
( ) Não

11. Os trabalhadores recebem orientações sobre o que é e como funciona o Sistema de Segurança da Informação da empresa? Se sim, de que forma?
( ) Sim, através de:
( ) treinamentos ( ) palestras
( ) reuniões ( ) outros
( ) Não

12. A empresa possui um servidor?
( ) Sim, quem tem acesso aos seus dados?
( ) todos os funcionários ( ) somente o suporte técnico
( ) somente a gerencia ( ) a gerencia e o suporte técnico
( ) Não

13. Existe algum sistema de backup das informações?
( ) Sim
( ) Não

14. Há nobreak ou geradores de energia, que garantam o suprimento de força quando há falta de abastecimento de energia?
( ) Sim
( ) Não

15. Na empresa há algum meio de detecção, prevenção e remoção de softwares maliciosos (vírus, spam, propagandas, etc.)?
( ) Sim, quais?
( ) antivírus ( ) bloqueadores de propagandas
( ) firewall ( ) outros
( ) Não

16. É feita uma vistoria nos equipamentos, em relação a programas instalados, vírus, funcionamento?

( ) Sim, com que frequência?
    ( ) apenas quando há algum problema ( ) mensalmente
    ( ) semanalmente ( ) anualmente
( ) Não

17. Existe um sistema de bloqueio de acesso relacionado ao uso da internet?
( ) Sim
( ) Não

18. Você considera a Informação como o principal ativo da sua empresa?
( ) Sim
( ) Não

19. Existe algum tipo de Política de Segurança da Informação sendo utilizada na empresa?
( ) Sim, ela possui uma certificação ISO?
    ( ) Sim
    ( ) Não
( ) Não

20.Você gostaria de possuir essa certificação?
( ) Sim
( ) Não, pois a empresa já possui uma certificação.