CENTRO UNIVERSITÁRIO UNIVATES
CURSO DE ANÁLISE DE SISTEMAS

ESTUDO SOBRE A APLICAÇÃO DA LEI DE ACESSO A INFORMAÇÃO, CONSIDERANDO A SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO NA PREFEITURA DE TRAVESSEIRO

JUNIOR RODRIGO WEIZENMANN

Lajeado, junho de 2015.

Junior Rodrigo Weizenmann

ESTUDO SOBRE A APLICAÇÃO DA LEI DE ACESSO A INFORMAÇÃO, CONSIDERANDO A SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO NA PREFEITURA DE TRAVESSEIRO

Projeto de pesquisa apresentado na disciplina de Trabalho de Curso II, do Curso de Análise de Sistemas, do Centro Universitário UNIVATES.

Orientador: Prof. Ms. Luis Antônio Schneiders

Lajeado, junho de 2015.

RESUMO

A evolução da tecnologia, que ocorre cada vez mais rápido, reflete-se na sociedade como também nas organizações tornando-se essencial para o desenvolvimento. Diante disso, a informação torna-se um bem imprescindível, sendo fundamental para a tomada de decisão. Dessa forma, as organizações obrigam-se a utilizar cada vez mais softwares e hardwares para tratar e cuidar das informações. Mas a utilização dessas tecnologias expõe as organizações e suas informações a riscos e vulnerabilidades, surgindo assim, uma preocupação com a segurança das mesmas, que muitas vezes são restritas e estratégicas. Portanto, as organizações são forçadas a procurar novos recursos que protejam as informações de vazamentos, perdas, acessos indesejados, entre outros. Esse estudo, que tem por objetivo verificar a atenção dada à segurança na área da Tecnologia da Informação da Prefeitura Municipal de Travesseiro e essa em relação à Lei12.527/2011, será abordado de forma quanti-qualitativa, apontando quais os pontos que inspiram maiores cuidados por não estarem sendo percebidos como fundamentais à segurança da informação.

Palavras-chave: Segurança da informação. Tecnologia da informação. Riscos e vulnerabilidade.

ABSTRACT

The evolution of technology, which is faster and faster, is reflected in society as well as in organizations, making it essential for development. Therefore, the information becomes an essential good, is central to the decision making. Thus, organizations are obliged to increasingly use software and hardware for treating and caring for information. But the use of these technologies exposes organizations and their information to risks and vulnerabilities arising thus a concern for their safety, which are often restricted and strategic. Therefore, organizations are forced to seek new means that protect information leaks, losses, unwanted access, among others. This study, which aims to verify the focus on security in the area of Information Technology of the City Hall of Travesseiro, and that in relation to Law 12.527/2011, will be addressed in quantitative and qualitative way, pointing the points which inspire greater care because they are not being perceived as fundamental to safety information.

Keywords: Information security. Information technology. Risks and vulnerability.

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS

ABNT – Associação Brasileira de Normas Técnicas

CGU – Controladoria Geral da União

CPD – Centro de Processamento de Dados

CPU – Central Processing Unit

GB – GigaBytes

HD – Hard Disk

IBGE – Instituto Brasileiro de Geografia e Estatística

IEC – International Eletrotechnical Commission

ISO – International Standards Organization

LAI – Lei de Acesso à Informação

MB – MegaBytes

NBR – Norma Brasileira

TI – Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO

A renovação e evolução das tecnologias a nível mundial, num ritmo cada vez mais rápido, teve seu reflexo na sociedade e nas organizações que desenvolveram-se nesse ritmo acelerado. Diante desse desenvolvimento, no qual a informatização está inserida, ela tornou-se essencial para as organizações, oferecendo-lhes um suporte para suprir as várias necessidades e dificuldades encontradas. Com isso, há a possibilidade de a organização se tornar mais competitiva, alcançando resultados favoráveis e obtendo maiores lucros. A globalização, que vem acompanhada de um mercado mais exigente, obriga as organizações a buscar uma melhor produtividade, como também, uma melhor qualidade tanto no produto como no serviço oferecido. Com isso, a evolução tornou a informação um bem precioso junto às organizações para tomada de decisões.

Nas organizações, a informação passou a ter um papel fundamental no desenvolvimento das mesmas, impactando diretamente para a tomada de decisões e servindo de sustentação da empresa no mercado, o que passa a ser um fator determinante para a sobrevivência da mesma. Em meio às disputas de um mercado cada vez mais acirrado, no que tange à qualidade, ao preço e outras variáveis, a informação torna-se imprescindível, pois deve ser completa, confiável, objetiva e rápida.

Diferente das organizações privadas, as organizações governamentais e sem fins lucrativos não utilizam as informações para obter lucro, mas, para reduzir os custos.

No entanto, na maioria das vezes não é isso que acontece. Quando não há uma preocupação na organização, as informações passam a ser desorganizadas e espalhadas, assim, dificultando sua utilização e atrasando a tomada de decisão. Percebendo este descaso e visando sanar tais falhas as empresas começaram a preocupar-se com recursos que controlam essas informações.

Cada vez mais as organizações estão dependentes das novas tecnologias, sendo quase impossível manter um negócio sem utilizar um software e hardware. Para que o funcionamento esteja de acordo com o que a empresa pretende e o mercado exige deve haver a integração entre homem e máquina. Os sistemas de informação passaram a ser incorporados nas organizações de tal maneira, que hoje são indispensáveis. São eles os responsáveis por reter os dados que são números e palavras soltas em informação. São muitos os benefícios que a tecnologia da informação traz à organização, principalmente quando utilizada como ferramenta diferencial de negócio.

O aumento expressivo de informações, com o aumento de recursos para controlar essas informações e a comunicação em redes de Internet e extranet, faz com que as organizações privadas e públicas se preocupem com a triagem das informações estratégicas. A utilização dessas, na gestão e a preocupação com a divulgação de informações restritas, vão gerando margens de insegurança. Essa preocupação obriga as organizações a procurar recursos, que as protejam de acessos indesejados, vazamentos e assédios à informação. Para isso ocorrer devem-se seguir normas, diretrizes, padrões e criar políticas de segurança.

Essas regras servem tanto para o setor privado quanto para o público. No setor público quanto mais perto da base, no caso o município, maior é a carência de segurança. Geralmente o ente público municipal é o mais vulnerável, isso por questões de recursos financeiros, técnicos e de estrutura.

Na Prefeitura Municipal de Travesseiro não é diferente. Sabe-se da responsabilidade de zelar e manter segura a informação. Mas, a carência de

estruturas adequadas, a falta de recursos financeiros e principalmente a não preocupação com a segurança, atrapalham a segurança da informação. Entretanto, é preciso gerar alternativas e recursos que permitam dar mais segurança e confiabilidade à Prefeitura. Para isso, torna-se necessário, elaborar uma política de segurança baseada em normas e diretrizes que auxiliem na segurança da informação, que é o propósito deste estudo.

Na sequência será apresentada a fundamentação teórica que abordará os conceitos de segurança da informação a qual servirá de base para a realização deste trabalho. Logo após serão apresentados os procedimentos metodológicos que definem o método de pesquisa a ser utilizado. O capítulo 4 que trata da caracterização da organização é um breve histórico da Prefeitura Municipal de Travesseiro, objeto da pesquisa. No capítulo 5 serão apresentados os dados e a análise das informações coletadas na entrevista realizada com os funcionários da organização. Por fim, serão apresentadas as considerações finais relacionando os resultados obtidos ao contexto real da organização em questão.

1.1 Definição do problema

Pertencendo à microrregião Lajeado/Estrela no Vale do Taquari, o município de Travesseiro, segundo o Censo 2010 IBGE tem uma população de 2.314 habitantes e sua economia baseada no setor primário. Como toda Administração pública, a Prefeitura Municipal de Travesseiro presta serviços aos seus munícipes. Entre os mais utilizados, estão: Educação, Saúde, Agricultura, Finanças e Obras. Todos esses setores geram algum tipo de informação, sendo de cunho público ou restrito.

As informações que são geradas na Secretaria Municipal da Educação são informações de cunho público, podendo ser divulgadas e servindo para cálculos estatísticos. Nas Secretarias Municipais de Obras e Agricultura a maioria delas, também é de caráter público, pois apresentam apenas dados sobre os serviços realizados servindo como estatística para o município. Já nas Secretarias Municipais

da Saúde e Finanças existem informações públicas, mas, a maioria delas são restritas e devem ser mantidas em sigilo. No caso da Secretaria Municipal da Saúde as informações geradas tratam de dados pessoais dos munícipes e em muitos casos sobre o estado de saúde dos mesmos. A Secretaria de Finanças gera informações, relacionadas às questões financeiras de pessoas físicas ou empresas, que podem até mesmo estar em débito com a Prefeitura, sendo restritas a esse setor.

Vários sistemas de informação que são utilizados diariamente nos diversos setores da Prefeitura Municipal, são disponibilizados pelos Governos Federal e Estadual, mas o principal sistema foi contratado pelo Município através de uma empresa terceirizada. Esse sistema de gestão pública abrange todos os setores, onde cada um possui seu módulo próprio.

Como nem todas as informações são de caráter público podendo ser divulgadas e acessadas, a situação da segurança da informação na Prefeitura Municipal de Travesseiro preocupa, pois muitas normas e diretrizes de segurança são ignoradas e não utilizadas. Assim, a segurança da informação torna-se vulnerável.

A informatização, além de benefícios, traz riscos e ameaças a uma organização. Na Prefeitura Municipal de Travesseiro não é diferente, pois com o aumento significativo de fraudes, golpes e acessos não autorizados, gera-se uma insegurança na gestão. Diante disso, surge a questão: Qual o grau de aderência da Prefeitura Municipal de Travesseiro à Lei de Acesso à Informação e à Norma NBR ISO/IEC 17799 e quais fatores comprometem a segurança da informação?

1.2 Objetivos

Os objetivos desse estudo foram divididos em geral e específicos.

1.2.1 Objetivo geral

Avaliar o grau de aderência da Prefeitura Municipal de Travesseiro em relação à Lei de Acesso à Informação considerando os elementos e as boas práticas pertinentes à segurança da informação, a qual apoia a aplicação desta lei.

1.2.2 Objetivos específicos

- Levantar os principais aspectos relacionados à segurança da informação;
- Analisar a Lei de Acesso à Informação;
- Analisar as condutas de segurança dos funcionários;
- Apontar fatores críticos relacionados à segurança de informação;
- Analisar o grau de aderência à norma NBR ISO/IEC 17799;
- Analisar o grau de aderência à Lei de Acesso à Informação;
- Identificar ameaças de segurança e de descumprimento da lei;
- Apontar fatores críticos relacionados à observância da Lei de Acesso à Informação.

1.3 Delimitação do estudo

Este estudo pretende avaliar a aderência à Lei de Acesso à Informação e a aderência à norma NBR ISO/IEC 17799 no que tange à segurança da informação na Prefeitura Municipal de Travesseiro, localizada no Vale do Taquari, estado do Rio Grande do Sul, no primeiro semestre de 2015.

1.4 Justificativa

Este estudo terá grande importância para Prefeitura Municipal de Travesseiro, pois serão identificados e apontados os riscos e as vulnerabilidades que afetam a segurança da informação dos diversos setores da organização. A Prefeitura por ser um órgão público dispõe de inúmeras informações importantes, próprias de sua estrutura como um todo, como também dos contribuintes municipais. Essas informações são de responsabilidade da Prefeitura, por isso faz-se necessário ter uma preocupação com a segurança das informações, para que não sejam perdidas, roubadas ou alteradas por pessoas mal-intencionadas ou por erros de usuários.

É importante salientar também, que após a realização desse levantamento, serão apresentadas propostas que poderão ser implementadas para reduzir os riscos e as vulnerabilidades da segurança da informação. Dessa maneira, a segurança da informação da Prefeitura Municipal de Travesseiro se tornará confiável, como também auxiliará no bom funcionamento da mesma e evitando prejuízos. Para que isso venha a ocorrer algumas medidas devem ser aplicadas na Prefeitura.

Com o uso da Internet estamos cada vez mais vulneráveis. O simples fato de utilizarmos as redes sociais faz com que estejamos nos expondo. Por isso, é preciso ter uma consciência sobre a segurança da informação. Este trabalho, por sua vez, visa a ampliação do conhecimento, direcionando a um melhor enfoque para os conceitos metodológicos sobre segurança da informação.

O estudo em questão visa aprofundar os conhecimentos do acadêmico, podendo servir como experiência e qualificação profissional. Por tratar-se de uma área pouco explorada e não havendo trabalhos acadêmicos sobre o assunto, este trabalho poderá servir de referência para estudos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Informação

Para Beal (2012), para entender o que é informação primeiramente é preciso entender o que é um dado. Dados podem ser entendidos como registros ou fatos em sua forma primária, não necessariamente física. Uma imagem guardada na memória também é um dado. A combinação ou organização de forma significativa desses registros ou fatos se transformam em uma informação. Conforme a autora informação consiste em dados coletados, organizados, orientados, aos quais são atribuídos significado e contexto.

Informação para Rezende (2003) é todo dado trabalhado, que se torna útil, tratado, o qual é atribuído e agregado um valor significativo, dando um sentido lógico para quem o utiliza.

A informação é um conjunto de dados processados e organizados que fazem sentido ao receptor da informação. As informações auxiliam na tomada de decisão. Quando for uma informação errada ou sem qualidade a decisão gerada também pode ser errada, ocasionando prejuízos a organização, Turban (2003).

2.1.1 Tipos de informação

Segundo Beal (2012), as organizações dependem de informações das diversas naturezas para alcançar os objetivos propostos. Aplicado em diferentes níveis organizacionais, elas podem ser classificadas em:

- Nível institucional: observa as variáveis nos ambientes externos e internos, monitorando e avaliando o desempenho das decisões de alto nível.
- Nível intermediário: observa as variáveis nos ambientes externos e internos, monitorando e avaliando o desempenho das decisões de nível gerencial.
- Nível operacional: possibilita executar suas atividades e tarefas, monitorando o espaço geográfico sob sua responsabilidade e subsidiar a tomada de decisões de nível operacional.

Rosini e Palmisano (2012), a informação é o elemento básico dos sistemas. Portanto, os conceitos básicos necessários dizem respeito às características da informação que se está trabalhando. O autor ressalta que apenas se trabalha com informação e não com dados. E existem tipos distintos de sistemas de informação, no qual cada um tem seus objetivos específicos.

Os sistemas são classificados conforme Rosini e Palmisano (2012) da seguinte maneira:

Sistemas de Informações Transacionais (operacionais) – SIT: é o sistema de mais baixo nível, atende as necessidades de nível operacional e serve como base para entrada de dados.

- Sistemas de Informações Especialistas, Sistemas de Automação – SE, SA: atende as necessidades de um grupo de especialistas da organização em qualquer nível, via de regra os especialistas, são pessoas com formação superior e participantes de grupos de trabalho muito especifico.
- Sistemas de Informações Gerenciais – SIG: atendem os níveis gerenciais de alto escalão, provendo relatórios gerenciais, que servem como base para o planejamento e tomada de decisão.

- Sistemas de Apoio a Decisão – SAD: atendem o nível estratégico da organização, sendo apoio para a direção da empresa na tomada de decisão.

2.1.2 Tecnologia da informação

A tecnologia encontra-se em toda parte. A vida atual é dominada por avanços tecnológicos tanto na sociedade quanto nas organizações. Os administradores sabem da necessidade de prever a mudança tecnológica e seu impacto sobre as suas atividades. Inovações radicais de tecnologia produzem transformações profundas na organização social, no trabalho e na própria vida cotidiana, conforme Rosini e Palmisano (2012).

Segundo Rezende (2003), a tecnologia da informação quando usada com o propósito de gerar e utilizar a informação em favorecimento da organização é denominado pelo autor de recurso tecnológico.

Rosini e Palmisano (2012) apud Goodman (1990), define a tecnologia como o conhecimento de relações causa-efeito embutido nas maquinas e equipamentos utilizados para realizar um serviço ou fabricar um produto.

A tecnologia da informação, conforme Rezende (2003) é composta por hardware, software, sistemas de telecomunicações e organização de dados e informação. É fundamental a presença do recurso humano, para a formação da Tecnologia da Informação.

A tecnologia não é muito mais que equipamentos e máquinas. A organização funciona a partir da operação de dois sistemas que dependem um do outro de maneira variada. Existindo o sistema técnico e o sistema social. Os dois sistemas serão otimizados, quando as necessidades de ambos serão atendidas, conforme Rosini e Palmisano (2012) apud Gonçalves (1994).

2.2 Sistema de informação

Um sistema é definido por De Sordi e Meireles (2010), como um conjunto de elementos interconectados, de tal modo que a transformação em uma de suas partes influencia todos os demais, havendo uma combinação causa efeito.

Para Rezende (2003), todo sistema utilizando ou não recursos tecnológicos de informação, que manipula e gera informação pode ser considerado um sistema de informação.

Atualmente a palavra “sistema” é mal empregada, usada de forma indiscriminada e sem qualquer critério, originando, em especial nos meios empresariais, a confusão de usá-la como definição e para expressar determinadas situações dentro de um software, segundo Rosini e Palmisano (2012).

Ainda para os autores, todo o sistema pode ser decomposto em partes menores denominadas de subsistemas. Onde eles são elementos interdependentes que integram para um objetivo comum, ajudando o sistema a atingir o objetivo maior, apresentando entrada de dados (imput), processamento e saída de informações (output).

Independentemente do tipo, nível ou classificação, o maior objetivo de um sistema é auxiliar nos processos de tomada de decisão. Isso não acontecendo sua existência não será significativa para a organização. Para isso o foco principal de um sistema deve estar direcionado para os objetivos da organização Rezende (2003).

Ainda para o autor, o sistema de informação traz benefícios incontestáveis para as organizações, sendo um diferencial de negócio, agregando valor à informação e facilitando a gestão.

Segundo De Sordi e Meireles (2010), um sistema é composto por vários componentes e autores que devem estar harmonicamente integrados. Sendo eles:

- Recurso de dados e informações: são um conjunto de caracteres armazenados que constituem dados e informações, com atribuições de tamanho, localização, seus usuários, data de criação, etc.

- Recurso de software: abrange todos os softwares necessários para o processamento dos algoritmos que constituem o sistema de informação.
- Recursos de tecnologia da informação: são processadores, meios de armazenamento, equipamentos para interação homem - máquina e outros dispositivos físicos que constituem um computador.
- Recursos de telecomunicações ou rede: são equipamentos e softwares específicos para a gestão e tráfego de dados e informações entre os computadores.
- Recursos humanos: são os profissionais da área da informática e de outras áreas técnicas como telecomunicação, responsáveis por construir, operar e aprimorar o sistema de informação. Além dos técnicos os clientes do sistema que são os usuários finais tem um papel importante neste contexto.

2.2.1 Sistema de conhecimentos

A informação, segundo Rosini e Palmisano (2012) é o elemento básico de um sistema, apenas se trabalha com informação e não com dados, pois o dado é a menor decomposição de um determinado elemento para a informação.

Para Rezende (2003), o conhecimento de uma organização é um processo interno de compreensão das informações recebidas, podendo resultar em ações completamente diferente como resultado de um mesmo conjunto de dados. Ele também pode ser visto como uma capacidade de agir e é contextual não podendo ser destacado do ambiente. Conforme o autor, sem fazer distinção entre tácito e explicito ou estabelecer duas dimensões para o conhecimento ele é reconhecido como uma mistura de elementos formalmente estruturados e intuitivos.

A geração do conhecimento ocorre quando as informações são comparadas, combinadas e analisadas por pessoas, principalmente quando utilizadas nos processos decisórios Rezende (2003).

Segundo o autor, os sistemas de conhecimentos, os sistemas de informação, a tecnologia da informação e as pessoas se constituem partes essenciais dos

desenvolvimentos recentes das estratégias empresariais baseadas em recursos e no conhecimento. Ainda para o autor, os recursos que são internos estão direcionados para a melhoria do desempenho da organização numa abordagem que propõe que os mesmos sejam os principais determinantes de sua competitividade inteligente, contemplando fatores da gestão do conhecimento.

Para Rezende (2003), os sistemas de conhecimento manipulam e geram conhecimento a partir das bases de dados, oriundas de dados do ambiente interno e externo da organização, criados por pessoas da organização e acionadas por meio dos recursos da tecnologia da informação.

2.2.2 Sistema de informação na gestão pública

Kanaane, (2010), os sistemas de informação estão transformando o ambiente de organizações públicas e privadas, levando aos cidadãos e aos gestores públicos informações rápidas e precisas. Existe uma similaridade entre os sistemas de informação de organização pública e privada, pois os dois setores produzem produtos e serviços para atender a demanda da sociedade.

As características sociais e culturais da organização, segundo Kanaane, (2010) são fundamentais e devem ser analisadas e compreendidas durante o processo de dimensionamento de sistema de informação. Deve ser observado o nível tecnológico e o processo de maturidade dos sistemas, pois, são importantes variáveis para automação de processos para a prestação de serviços on-line ao cidadão.

As organizações públicas e privadas são regidas por leis municipais, estaduais e federais, devendo assim adequar seus sistemas para operarem de maneira global sem perder suas características e a integração de dados e processos nos quais estão inseridos, Kanaane (2010).

Além de projetar sistemas que possam prover serviços à sociedade as organizações públicas precisam proporcionar aos gestores públicos informações necessárias para a gestão dos processos e tomada de decisões baseadas em

analises e fatos. Para o autor, as organizações precisam ainda controlar seus sistemas de informação para compreender processos.

Conforme Kanaane, (2010), os sistemas de informação em áreas governamentais constituem questões estratégicas, questões de segurança e a governança do Estado, tendo o sistema um papel importante na sociedade e nas organizações públicas e privadas.

2.3 Política de segurança da informação

Quando se pensa em segurança de informação, a primeira ideia que vem a mente é a proteção das informações, independente onde estejam (papel, memória de computador ou trafegando pela linha telefônica). Conceitualmente, um computador ou sistema computacional é considerado seguro se houver garantia de atuar exatamente como o esperado Dias, (2000).

Com o propósito de fornecer orientação e apoio às ações de gestão de segurança, para Sêmola (2003) a política de segurança da informação é fundamental para a organização, sendo similar à constituição federal para um país. Desta forma, assume uma grande abrangência e por conta disso, é subdividida em três blocos: diretrizes, normas, procedimentos e instruções.

Conforme o autor deve-se estabelecer padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança estabelecido para a empresa, devendo a política ser personalizada.

Para Beal (2008), a Política de Segurança da Informação (PSI) na organização, deve ser observada por todos os seus integrantes e colaboradores e aplicada a todos os sistemas de informações e processos corporativos.

As diretrizes que por si só tem papel estratégico, precisam expressar a importância que a organização dá para a informação, além de comunicar aos

funcionários seus valores e seu comprometimento em incrementar a segurança à sua cultura organizacional, Sêmola (2003).

Segundo Beal (2008), a política de segurança da informação, deve abranger amplamente com foco nas questões de princípio não detalhando aspectos técnicos e de implementação.

Ainda a autora, embora o conteúdo da política depende do tamanho da organização, ela deverá abranger sempre que cabível os seguintes aspectos:

- Organização da segurança: definir o responsável pela segurança da informação em todos os níveis da organização e quais as linhas hierárquicas existentes entre as funções de segurança.
- Segurança do ambiente físico: normas de proteção contra o acesso não autorizado aos recursos e instalações de processamento de informações evitando danos e interferência.
- Segurança do ambiente lógico: diretrizes para proteger a integralidade dos serviços, realizando operações seguras e corretas.
- Segurança das comunicações: diretrizes para proteger dados e informações durante os processos de comunicação.

2. 4 Segurança da informação

Segurança da informação segundo Fontes (2006) é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação.

Para Sêmola (2003), segurança da informação é uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Ainda o autor, considera como a prática de gestão de riscos de incidentes que impliquem no comprometimento dos três principais conceitos de segurança: confidencialidade, integralidade, legalidade e disponibilidade da informação. Conforme o autor, esses conceitos são responsáveis

sobre todos os momentos do ciclo de vida da informação, através do manuseio, armazenamento, transporte e descarte.

Conforme Fontes (2006), proteger a informação significa garantir:

- Disponibilidade: a informação deve estar acessível para o funcionamento da organização e para o alcance de seus objetivos.
- Integralidade: a informação deve ser verdadeira, correta e não estar corrompida.
- Confidencialidade: a informação deve ser acessada e utilizada exclusivamente pelos que necessitam dela para a realização de suas atividades profissionais na organização, havendo uma autorização previa.
- Legalidade: o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos bem como com os princípios éticos seguidos pela organização e desejados pela sociedade.

Além de confiabilidade, integralidade e disponibilidade, para Beal (2008), alguns aspectos adicionais de segurança emergem quando a informação precisa ser transmitida num processo de comunicação. Conforme a autora, problemas como a alteração fraudulenta de documentos em trânsito e disputas sobre a origem de uma comunicação ou o recebimento de uma informação transmitida precisam ser equacionados, levando a necessidade de estabelecer alguns objetivos adicionais relativos à segurança da comunicação.

Albuquerque e Ribeiro (2002), problemas de segurança é a perda de qualquer aspecto da segurança para o sistema, como confidencialidade ou integralidade dos dados. Mas, para os autores, alguns problemas são causados por desastres naturais, inundações, furacões, tempestades, etc. entre outros fatores como sinistros, ataques terroristas etc. Tudo isso deve ser levado em conta na hora de planejar a segurança de um sistema.

Outros problemas encontrados na segurança ocorrem devido ao uso incorreto do sistema, isso por parte do usuário e do administrador cometendo erros Albuquerque e Ribeiro (2002).

Para Dias (2000), existem duas formas de abordar a segurança física, que através da segurança do acesso o qual adota medidas impedindo o acesso físico não autorizado e a segurança ambiental que evita danos por causas naturais. Ainda a autora, segurança de acesso físico, deve se basear em perímetros predefinidos e com acesso restrito de acordo com a função desempenhada na organização.

Segundo o autor, os equipamentos como: servidores, CPU's, estações de trabalho, etc. devem ser diretamente protegidos pelo controle de acesso físico.

2.4.1 Backup

Para Fontes, (2006), se uma informação for destruída e não tiver uma cópia de segurança (backup), nunca mais será recuperada. Isso vale tanto para a informação armazenada no ambiente de tecnologia como as registradas em papel. A destruição pode ser por erro ou de forma intencional.

Para o autor, no ambiente de tecnologia, as informações podem ser alvo de ações criminosas, mas, apesar da perda da mídia ser por má-fé, geralmente a perda da informação acontece por erro. Independentemente do que motivou a perda da informação, a organização precisa estar apta a recuperar essa informação. Uma cópia deve estar segura e protegida adequadamente, para que em casos de perda ou destruição dessa informação tenha um modo de recuperá-la.

Dias (2000), o backup é um dos itens mais importantes em um plano de contingência na área da informática, mas, não faz sentido manter um plano para recuperação se não haverem dados para serem recuperados. Conforme a autora é fundamental ter backups atualizados e completos no momento que ocorrer algum problema. No caso de perdas totais de equipamentos, os backups podem ser restaurados em outros equipamentos, não gerando danos às informações da empresa.

Os procedimentos que estão inseridos na política de backups devem ser seguidos rigorosamente para não causar danos às informações. A definição dos

critérios das copias, devem ser definidos pelos responsáveis do sistema, gerência e usuários mais críticos. Assim a política de backup, também define o grau de importância do sistema, Dias (2000).

Conforme Fontes, (2006), uma ação simples, de baixo custo e de alta eficácia, pode ser feita: realizar backups periodicamente irá minimizar impactos nas organizações caso venha acontecer à destruição da informação. Várias são as maneiras de realizarmos um Backup. Os arquivos podem ser salvos em cd's, pen drive, hd's externos, computadores em rede, em nuvens, entre outros mecanismos.

2.4.2 Firewall

Firewall, para Beal (2008), é uma das ferramentas mais utilizadas e citadas na segurança de redes. Ele consiste basicamente numa barreira de proteção entre um computador ou uma rede interna e seu ambiente externo, bloqueando informações que não atendem critérios predefinidos de segurança.

Os sistemas tradicionais de redes sem firewall, normalmente permitem acesso direto ao mundo externo, se conectando com qualquer máquina conectada na rede de computadores e vice-versa. Tornando-se frágil, pois a existência de um único computador sem proteção compromete toda segurança da rede Dias (2000).

Conforme a autora a falta de proteção, permite o acesso de invasores a partir daquele computador inseguro, causando transtornos a organização, capturando senhas de acesso e alterando configurações. Torna-se algo difícil de administrar em termos de segurança como também se torna quase impossível detectar uma invasão.

Como novas formas de ataques são descobertas diariamente, não é possível configurar um firewall uma vez e torná-lo efetivo contra ameaças por tempo indeterminado, ele deve sofrer manutenção e atualizações constantes Beal (2008).

Dias (2000), acredita que um firewall instalado corretamente e configurado é capaz de reduzir os riscos de invasão em pelo menos 20 %. Porém, antes de se

conectar ao mundo externo, outras medidas de segurança da informação devem ser seguidas.

2.4.3 Criptografia

Albuquerque e Ribeiro (2002) define a criptografia como um processo pelo qual uma informação ou um texto é embaralhado de forma que só seja possível a obtenção do texto original aplicando-se uma operação baseada através de uma chave de acesso. Para os autores, para obtermos as informações originais precisamos saber qual a operação para decriptografia e a chave de acesso.

A criptografia para Albuquerque e Ribeiro (2002), serve de base a uma serie de mecanismos de segurança, sendo que muitas funcionalidades de segurança só são possíveis com o uso da criptografia. Ela protege os dados e informações, provendo sigilo sobre arquivos armazenados em diretórios ou partições de discos.

Conforme os autores, basicamente existem dois tipos de criptografia: simétrica e a assimétrica.

- Simétrica: utiliza uma chave para criptografar os dados e a mesma chave é utilizada para decriptografá-los, obtendo assim os dados originais novamente.
- Assimétrica: ela sempre produz as chaves em par, assim que uma chave é utilizada para criptografar, apenas a outra chave pode ser usada para decriptografar e assim obter as informações e dados originais.

2.5 ABNT NBR ISO/IEC 17799: 2005

A informação, processos, sistemas e redes são fundamentais para os negócios da organização. Assim como a integridade, confidencialidade e disponibilidade da informação são essenciais para preservar a competitividade e a lucratividade da organização no mercado.

A norma NBR ISO/IEC 17799, fornece recomendações para gestão da segurança da informação aos responsáveis pela introdução, implementação ou manutenção da segurança em suas organizações. Na qual essa Norma pode ser usada como ponto de partida para recomendações para a organização. Tem como propósito prover uma base comum para o desenvolvimento de normas de segurança organizacional e das práticas efetivas de gestão da segurança, e prover confiança nos relacionamentos entre as organizações.

Conforme a NBR ISO/IEC 17799, é essencial que a organização identifique os requisitos de segurança, através da avaliação de riscos dos ativos da organização, identificando as ameaças aos ativos mais vulneráveis. É importante que a organização identifique os requisitos sobre a legislação vigente, estatutos, contratos e regulamentações com os prestadores de serviço. Suas operações devem ter apoio de objetivos e requisitos para o processamento da informação.

NBR ISO/IEC 17799, prevê uma política de segurança da informação na organização, estabelecendo regras claras com a segurança. Sendo documentado e aprovado pela direção, publicado e comunicado de forma clara a todos os funcionários.

Na fase de recrutamento de recursos humanos a segurança deve ser observada para reduzir riscos de erro humano, roubo, fraude e uso indivíduo das instalações. Dependendo dos casos devem ser feitos acordos assinados de confidencialidade seguindo as políticas de segurança da organização. Treinamentos e educação em segurança da informação devem ser regulares de forma a minimizar possíveis riscos de segurança.

A Norma estabelece regras sobre a proteção de instalações e equipamentos, protegendo-os fisicamente contra ameaças e perigos ambientais como também a acessos não autorizados. É preciso que sejam adotados controles para minimizar ameaças, incluindo: fogo, água, roubo, interferência no fornecimento de energia entre outros.

Além da proteção é fundamental a realização de manutenções periódicas dos equipamentos, garantindo a continuidade, disponibilidade e integralidade dos mesmos.

Conforme a NBR ISO/IEC 17799, são estabelecidas normas para controlar o acesso dos funcionários, para prevenir o acesso não autorizado aos sistemas de informação e as instalações. Devem ser estabelecidos procedimentos formais para controlar a concessão de direitos de acessos aos sistemas de informação e serviços.

Um gerenciamento de senhas deve ser realizado, solicitando declarações assinadas pelos usuários a fim de manter a confidencialidade de sua senha, além de utilizar outras tecnologias para a identificação dos usuários.

Para proteger a informação, cópias de segurança (backups) devem ser feitos regularmente, e recursos e instalações alternativas devem ser disponibilizadas de forma a garantir que todos os dados e sistemas essenciais possam ser recuperados após desastres ou problemas adversos. Para isso convém que os backups sejam testados regularmente para garantir a continuidade do negócio.

2.6 Lei de acesso à informação

A primeira nação no mundo a desenvolver um marco legal sobre acesso a informação foi a Suécia, em 1766. Na América Latina, a Colômbia foi pioneira ao estabelecer, em 1888, um Código que franqueou o acesso a documentos de Governo. Já a legislação do México, de 2002, é considerada uma referência, tendo previsto a instauração de sistemas rápidos de acesso, a serem supervisionados por órgão independente. Chile, Uruguai, entre outros, também aprovaram leis de acesso à informação (CGU, 2013).

Através da Constituição da República Federativa do Brasil de 1988, por exemplo, colocou o direito de acesso a informações públicas no rol de direitos fundamentais do indivíduo. De início, já no Título I - Dos Direitos e Garantias Fundamentais, Capítulo I – Dos Direitos e Deveres Individuais e Coletivos, foi previsto no art. 5º, incisos XIV e XXXIII.

Com a promulgação da Constituição de 1988, várias leis, decretos e portarias que trataram do acesso às informações públicas foram publicados. Se destacando a Lei de Responsabilidade Fiscal ou Lei Complementar nº 101/2000 e a Lei Complementar 131/2009, como também a criação do Portal da Transparência pelo Poder Executivo Federal em 2004. Todas essas leis e decretos contribuíram para que se iniciasse no ano de 2009 a discussão sobre a Lei de Acesso a Informação que foi sancionada em 18 de novembro de 2011 sob nº 12.527.

A Lei 12.527/2011 entrou em vigor em 16 de maio de 2012, devendo ser cumprida pelos órgãos e entidades públicas dos três Poderes (Executivo, Legislativo e Judiciário), de todos os níveis de governo (federal, estadual, distrital e municipal), assim como os Tribunais de Contas e o Ministério Público, bem como as autarquias, fundações públicas, empresas públicas, sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Essa Lei estabelece que, órgãos e entidades públicas devem divulgar informações de interesse coletivo, salvo aquelas cuja confidencialidade esteja prevista no texto legal. Isto deverá ser feito através de todos os meios disponíveis e obrigatoriamente em sítios da internet.

A Lei 12.527/2011 prevê exceções à regra de acesso para dados pessoais e informações classificadas por autoridades como sigilosas. Informações sob a guarda do Estado que dizem respeito à intimidade, honra e imagem das pessoas, por exemplo, não são públicas, ficando protegidas por um prazo de cem anos. Elas só podem ser acessadas pelos próprios indivíduos e, por terceiros, apenas em casos excepcionais previstos na Lei (CGU, 2013).

O funcionário que cometer conduta ilícita, será responsabilizado pelo ato, podendo caracterizar infração ou improbidade administrativa.

2.7 Controle de acesso

No ambiente atual de interligações em redes, os problemas de segurança aumentam significativamente. Atualmente qualquer usuário com um microcomputador se torna um “administrador de sistema”, sendo que um pequeno descuido pode tornar toda rede vulnerável Beal (2008).

Para Dias (2000), o controle de acesso tanto físico como lógico, tem como objetivo proteger os recursos tecnológicos contra perdas, danos, modificações ou divulgação não autorizada. Conforme a autora, os sistemas computacionais são de difícil controle, ainda mais se estiverem conectados a redes locais ou de maior abrangência.

O controle de acesso às informações, softwares e dados dependem do desenvolvimento e implementação de políticas de segurança da informação. Essa responsabilidade é do administrador de segurança da informação que deve supervisionar e implementar todas as políticas de acessos, Imoniana (2010).

Ainda para o autor, a segurança de acesso lógico é a proteção dada pelos recursos tecnológicos de um sistema, que proíbe o acesso não autorizado aos dados e informações de usuários específicos. Essa segurança tem como principal aliado a identificação através de senhas, identificando cada usuário no sistema.

As senhas de acesso, segundo Beal (2008) devem estar sujeitas a processos formais de concessão, alteração e armazenamento. A entrega de senhas temporárias, que obrigam a troca, auxilia no controle usado para melhorar a segurança.

Dias (2000), ressalta que mesmo com controles sofisticados, o ponto fraco sempre será o usuário. Pois, o descuido no compartilhamento de senhas, na proteção de informações confidenciais ou a escolha de senhas que facilmente são descobertas comprometem a segurança da informação.

Segundo a autora, a conscientização e um bom treinamento aos funcionários, são fundamentais para que a estratégia de controle de acesso seja eficaz e uma das melhores maneiras de garantir a segurança da informação.

O controle de acesso físico, segundo Beal (2008), requer maneiras de barrar pessoas não autorizadas a terem acessos à informação. Para isso devem ser utilizados os controles:

- Identificação dos funcionários através de crachás com fotos, por exemplo;
- Identificação dos visitantes, registrando entradas e saídas;
- Uso de cartões PIN, para validar e registrar o acesso à informação e instalações sensíveis;
- Estabelecer regras de acesso às áreas de segurança e atualização periódica da concessão de direitos de acesso;
- Orientações aos funcionários para informar à segurança sobre a presença de estranhos não identificados.

Para autora esses são alguns itens que diminuem os riscos à segurança da informação nas organizações.

2.8 Auditoria

Dias (2000) conceitua a auditoria como uma atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais de uma determinada organização. Ela tem a finalidade de verificar a conformidade com os objetivos, políticas, normas, padrões e orçamentos da organização.

Para auditar as informações em ambientes de tecnologia de informação o auditor pode desenhar as abordagens que lhe convêm. Sendo as mais comuns as abordagens ao redor do computador, através do computador e com o computador. Para o autor, a auditoria sempre foi conhecida por sua responsabilidade nos testes de confiabilidade dos registros de acordo com os documentos originais, Imoniana (2010).

Conforme o autor, devido os avanços tecnológicos, que interferem diretamente nas tecnologias gerenciais é necessário guardar as informações para que sejam acessíveis para auditoria quando forem requisitados.

Para Albuquerque e Ribeiro (2002), realizar uma auditoria num sistema se torna nada simples. Simples é implementar, mas, o difícil é projetar num sistema. É preciso ver o que realmente interessa para ser auditado, que ações devem ser registradas. Se registrar informações, tudo poderá interferir no desempenho do sistema, por haver informações demais. Para os autores, se registrar poucas informações, existe o risco de não registrar as informações que podem desvendar um problema.

O órgão fiscalizador da auditoria pode ser interno, realizado por um departamento interno da organização ou externo, sendo realizada por instituições independentes e articulada, realizando um trabalho conjunto entre auditoria interna e externa, Dias (2000).

Para a autora, os membros da equipe de auditoria devem ter certo conhecimento para planejar, dirigir, supervisionar e realizar o trabalho, como também experiência prática anterior.

3 PROCEDIMENTO METODOLÓGICO

3.1 Tipo de pesquisa

Pesquisa é um procedimento racional sistemático que tem como objetivo proporcionar respostas aos problemas que são propostos, sendo desenvolvida mediante os conhecimentos disponíveis, utilizando métodos e técnicas, (Gil 2002).

3.1.1 Definição da pesquisa quanto aos seus objetivos

Para Gonçalves (2004), quando não se conhece bem o problema de pesquisa que será investigado, mas existem suspeitas e sintomas, o caminho pode ser a elaboração de uma pesquisa exploratória.

Para este trabalho será utilizado a pesquisa exploratória, a qual abordará uma área pouco explorada, buscando informações restritas sobre a segurança da informação da Prefeitura Municipal de Travesseiro. Exigindo um estudo minucioso para obter informações do objeto pesquisado.

Segundo Vergara (2007), a pesquisa exploratória não deve ser confundida com leitura exploratória. É realizada em área na qual existe pouco conhecimento sistematizado e acumulado. Conforme Gil (2002), ela tem como objetivo

proporcionar maior familiaridade com o problema, tornando-o mais explícito. Dando a pesquisa um aprimoramento de ideias ou a descoberta de intuições. Para o autor, o seu planejamento é bastante flexível, possibilitando considerações dos mais variados aspectos relativos ao fato do estudado.

Para Gil (2002), na maioria dos casos as pesquisas exploratórias envolvem levantamentos bibliográficos, entrevistas com pessoas que tiveram experiência prática com o assunto de estudo e analises de exemplos que estimulem a compreensão do assunto. Mesmo sendo bastante flexível, o planejamento na maioria dos casos assume forma de pesquisa bibliográfica ou de estudo de caso.

Propondo a busca dos elementos necessários para averiguar a segurança da informação da Prefeitura Municipal de Travesseiro, serão apresentados os dados do estudo. Segundo Gil (2012) o produto final deste processo passa a ser um problema mais esclarecido, ajudando na compreensão do problema.

3.1.2 Definição da pesquisa quanto à natureza da abordagem

A pesquisa será de natureza quanti-qualitativa, que auxiliará na abordagem dos dados coletados sobre a aderência à Lei de Acesso à Informação e à norma NBR ISO/IEC 17799 na Prefeitura Municipal de Travesseiro. Ela dará valor e utilidade a esses dados, de forma organizada, permitido uma melhor definição de escopo e foco do estudo.

Segundo Sampieri (2006), a pesquisa com:

> [...] enfoque quantitativo utiliza a coleta e a análise de dados para responder às questões de pesquisa e testar as hipóteses estabelecidas previamente, e confia na medição numérica, na contagem e frequentemente no uso de estatística para estabelecer com exatidão os padrões de comportamento de uma população.

Já a pesquisa qualitativa, para Roesch (1996) é apropriada para a avaliação formativa, quando se trata de melhorar a efetividade de um programa ou plano, selecionando metas de um programa e construir uma intervenção.

Conforme Creswell (2007), a pesquisa qualitativa, emprega diferentes alegações de conhecimento, estratégias de investigações e métodos de coleta de dados. Os procedimentos qualitativos, embora sejam similares aos quantitativos, se baseiam em dados de texto, imagens e usam estratégias diversas de investigação.

Gibbs (2009), os dados qualitativos são essencialmente significativos, mas, além disso, mostram grande diversidade. Não são inclusos em contagens e medidas, mas, praticamente qualquer forma de comunicação humana, como: escrita, auditiva ou visual, por comportamentos, simbolismo ou artefatos culturais.

3.1.3 Definição da pesquisa quanto aos procedimentos técnicos

Os procedimentos técnicos que serão utilizados para a realização desta pesquisa, será a pesquisa bibliográfica, pesquisa documental e estudo de caso.

a) Pesquisa bibliográfica

A pesquisa bibliográfica é desenvolvida com base de material já elaborado constituído principalmente de livros e artigos científicos. Sendo exigido em quase todos os estudos dessa natureza. Boa parte dos estudos exploratórios pode ser definida como pesquisa bibliográfica Gil (2002).

Para Vergara (2007), é um material acessível ao público em geral, e fornece instrumental analítico para qualquer outro tipo de pesquisa, mas também pode se esgotar em si mesma. O material pode ser de fonte primária, quando escrito por um autor ou secundária, quando aparece editado em redes eletrônicas ou em outros livros.

b) Pesquisa documental

A pesquisa documental, conforme Gil (2002), assemelha-se muito a pesquisa bibliográfica, a diferença essencial entre as duas está na natureza das fontes. A pesquisa documental vale-se de matérias que ainda não receberam um tratamento

analítico, ou que ainda podem ser reelaborados de acordo com os objetos da pesquisa.

Para Gil (2012), há que se considerar que na pesquisa documental, o primeiro passo consiste na exploração das fontes documentais, sendo elas em grande número. Existindo os documentos de primeira mão, que não receberam tratamento analítico, que são: documentos oficiais, reportagem de jornal, cartas, contratos, fotografias, gravações, etc. E os documentos de segunda mão, esses já analisados de alguma forma, tais como: relatórios, tabelas, etc.

c) Estudo de caso ou exploratório

Os estudos de caso para Gil (2012), são caracterizados pelo estudo profundo e exaustivo de um ou de poucos objetos, permitindo seu conhecimento amplo e detalhado, tarefa praticamente impossível mediante os outros tipos de delineamentos considerados.

O estudo de caso é usado em muitas situações, contribuindo para o nosso conhecimento de fenômenos individuais, grupais, sociais, políticos, organizacionais e relacionados. Permite que os investigadores retenham as características holísticas e significativas dos eventos analisados, Yin (2010).

Conforme o autor, o estudo de caso é um estudo empírico que investiga um fenômeno atual dentro do seu contexto de realidade, quando as fronteiras entre o fenômeno e o contexto não são claramente definidas e no qual são utilizadas várias fontes de evidência.

Em Yin (2010), o protocolo de pesquisa é uma maneira de aumentar a confiabilidade do estudo de caso, se destinando a orientar o investigador na realização da coleta de dados. Esse protocolo deve conter as seguintes seções:

- Uma visão geral do projeto do estudo de caso;
- Procedimentos de campo;
- Questões do estudo de caso;
- Um guia para o relatório do estudo de caso.

3.2 Unidade de análise

A unidade de análise a ser pesquisada é o setor de Tecnologia da Informação da Prefeitura Municipal de Travesseiro. O estudo será baseado na análise da segurança da informação e abrangerá todos os setores que fazem uso de sistemas de informação.

As informações para o desenvolvimento da pesquisa serão provenientes de entrevistas, questionários e observações aplicadas para oito funcionários que trabalham nos diferentes setores da Prefeitura.

3.3 Definição do plano de coleta

Para Vergara (2007), na coleta de dados deve ser informado como eles serão obtidos para responder ao problema.

Na coleta de dados, serão levantados os principais aspectos relacionados à segurança da informação. Isso se dará através da pesquisa bibliográfica. Conforme Gil (2002) a pesquisa bibliográfica é desenvolvida com base em material já elaborado constituído principalmente de livros e artigos científicos. Sendo exigido em quase todos os estudos dessa natureza.

Também será realizada uma análise dos sistemas de informação utilizados, e serão identificados os recursos de segurança utilizados na Prefeitura de Travesseiro. Essa coleta será baseada em pesquisa documental e entrevistas com funcionários dos setores. Para Gil (2002) a pesquisa documental vale-se de matérias que ainda não receberam um tratamento analítico, ou que ainda podem ser reelaborados de acordo com os objetos da pesquisa. A entrevista, conforme Lakatos e Marconi (2010), é a troca de informações entre duas pessoas, a fim de que uma delas obtenha informações sobre determinado assunto, sendo ideal para investigar acontecimentos afins à ciência.

A conduta de segurança dos funcionários será analisada através do método da observação, entrevista e questionário, e, segundo Vergara (2007) a observação pode ser simples ou participante. Na simples o pesquisador mantém certo distanciamento do grupo ou da situação, sendo apenas um espectador não interativo. Já na participante o pesquisador é um ator ou um expectador interativo.

O estudo de caso servirá para apontar fatores críticos e propor uma estrutura à segurança da informação. Permitindo que os investigadores retenham as características holísticas e significativas dos eventos analisados, Yin (2010).

3.4 Definição do plano de tratamento dos dados

As perguntas abertas em questionários são a forma mais elementar de coleta de dados qualitativos. O pesquisador deve formular questões que permitam a entender e capturar a perspectiva dos respondentes. A qualidade da resposta depende da habilidade de redação da pessoa em responder o questionário, Roesch (2005).

A autora destaca, que enquanto as respostas para perguntas fechadas em questionários são fáceis de codificar, o mesmo não acontece em perguntas abertas. Quando se dá liberdade ao respondente, respostas inesperadas surgem. Elas deverão ser categorizadas para possibilitar sua interpretação.

Conforme Roesch (2005), por outro lado o método de observação traz o pesquisador até o local do evento, permitindo uma análise de profundidade e detalhes.

Para Yin (2010), o protocolo de pesquisa é uma maneira de aumentar a confiabilidade do estudo de caso, se destinando a orientar o investigador na realização da coleta de dados. Esse protocolo contempla uma visão geral do projeto, procedimentos de campo, questões de estudo e um guia para relatórios.

Através da organização das informações que serão coletadas e com os materiais pesquisados será realizada uma análise que tem como objeto, elencar as

prioridades da segurança da informação da Prefeitura e alcançar o objetivo geral deste estudo.

3.5 Limitação do método

Todo método tem possibilidades e limitações. É preciso antecipar-se as críticas que o leitor poderá fazer ao estudo, explicitando as limitações que o método escolhido oferece, mas que ainda assim o justificam como o mais apropriado ao estudo, Vergara (2007).

Conforme Roesch (2005) podem existir limitações, desde a dificuldade de entendimento das questões por parte do entrevistado, o cuidado por parte do entrevistador em não influenciar o entrevistado, a falta de confiança no entrevistador e o tempo necessário para a realização.

Vários fatores podem limitar a pesquisa. Por se tratar de um órgão público poderão ser negadas algumas informações, impossibilitando assim o acesso a elas. O tempo poderá ser limitado, como também poderá faltar informações por elas não serem guardadas.

4 CARACTERIZAÇÃO DA ORGANIZAÇÃO

Pertencendo à microrregião Lajeado/Estrela no Vale do Taquari, o município de Travesseiro no ano de 1991, ainda distrito do município de Arroio do Meio, cria uma comissão de emancipação. Em 20 de março de 1992, foi sancionado o Decreto nº 9596, que cria o município de Travesseiro e em 1º de janeiro de 1993 é oficialmente instalado.

Com uma receita de R$ 11.000.000,00 anuais, sua economia está baseada na produção primária que representa 80% da receita. Conforme censo 2010 do IBGE, Travesseiro possui 2.314 habitantes, esses 1.427 residem na zona rural e 887 na zona urbana do município.

No prédio da prefeitura funcionam as Secretarias da Administração e Finanças, Educação, Cultura, Turismo, Desporto e Planejamento. O município possui um Centro Municipal de Saúde onde funciona a Secretaria da Saúde e Assistência Social. Já a Secretaria de Obras está alocada junto ao prédio do parque de máquinas e a Secretaria da Agricultura e Meio Ambiente funcionam em um prédio alugado.

Como toda administração pública, a Prefeitura Municipal de Travesseiro presta serviços aos seus munícipes, nos diferentes setores. Utilizando diariamente vários sistemas de informações, disponibilizados pelo Governo Federal, Estadual, Bancos e um sistema próprio de gestão pública, desenvolvido por uma empresa privada.

A atual infraestrutura de TI é composta por:

- Servidor da marca IBM com Processador Intel *Xeon Six Core* Modelo E5-2420 1.9GHz/1333MHZ/15MB, 8GB e dois HD's de 500GB, sistema operacional *Linux*;
- *Switch* da marca Intelbras de 24 portas;
- *Nobreak* da marca NHS, 2,2 Kva;
- Dois roteadores *Wireless TP-Link*, um de 150 Mbps e outro de 300 Mbps.

A infraestrutura é adequada para o funcionamento do *software* de gestão pública, do *firewall* que gerencia a rede e o Portal da Transparência que serve para disponibilização das informações da Prefeitura Municipal na internet.

5 APRESENTAÇÃO E ANÁLISE DOS DADOS

Neste capítulo são apresentados e analisados os resultados da pesquisa do grau de conformidade à norma NBR ISO/IEC 17799, e a Lei 12.527/2011 – Lei de Acesso à Informação, obtidos na Prefeitura Municipal de Travesseiro, através dos métodos descritos no capítulo 3 deste trabalho.

Primeiramente são apresentados e analisados os dados referentes ao Grau de Aderência da Prefeitura Municipal de Travesseiro em relação à NBR ISO/IEC 17799, os quais foram obtidos a partir de um questionário especifico aplicado ao responsável da área de TI desta organização (Apêndice A).

Na segunda etapa são apresentados e analisados os dados que se referem à aderência da Prefeitura Municipal de Travesseiro a Lei 12.527/2011 que é a Lei de Acesso a Informação. Para tanto, foi criado um questionário, o qual foi aplicado para oito servidores, representantes dos setores da Prefeitura, conforme (Apêndice B)

É realizada também uma terceira etapa, na qual os dados resultantes das duas etapas anteriores são cruzados e apresentados na Tabela 5. Deste modo objetivando a identificação do Grau de Aderência da Lei de Acesso a Informação em relação à norma NBR ISO/IEC 17799, visando à identificação de uma possível análise da real situação da organização.

5.1 O grau de aderência à norma NBR ISO/IEC 17799

Conforme Sêmola (2003), o objetivo da análise do grau de aderência é permitir a percepção do nível de segurança em TI em relação aos controles sugeridos pela norma NBR ISO/IEC 17799. É um diagnóstico simples e rápido, baseado em perguntas objetivas com pontuação associada que irá revelar os níveis de segurança aplicados na organização.

O quadro 1 demonstra a pontuação utilizada para a classificação do grau de aderência a ser atribuída a cada quesito da norma segundo o resultado do questionário.

Quadro 1 – Grau de aderência - Tabela de Pontuação.

Resposta A (Sim): some 2 pontos. Resposta B (Sim, porém desatualizado): some 1 ponto. Resposta C: (Não) não some, nem subtraia pontos.

Fonte: (Sêmola, 2003)

Sêmola (2003), a abordagem deve ser realizada com base na norma NBR ISO/IEC 17799, seguindo os 10 quesitos de segurança da informação, conforme apresentados abaixo.

5.1.1 Política de segurança da informação

A política de segurança da informação tem como objetivo prover orientação, apoiando a direção da organização para a segurança da informação de acordo com os requisitos do negócio e com as leis regulamentares vigentes. Deve ser estabelecida uma clara orientação da política alinhada com os objetivos do negócio com a segurança da informação por meio de publicações para toda organização (NBR ISO/IEC 17799, 2005).

Quadro 2 – Política de segurança da informação.

Prática	Aderência		
	Sim	Sim, porém desatualizada	Não
Política de segurança?			X
Algum responsável pela gestão da política de segurança?			X

Fonte: do autor, 2015, teste de conformidade (Sêmola, 2003).

O Quadro 2 demonstra que a política de segurança da informação da Prefeitura de Travesseiro não está aderente à norma, evidenciando a inexistência de uma Política de Segurança da Informação e a falta de documentação ou diretrizes que regulamentam a segurança da informação da organização.

5.1.2 Segurança organizacional

Conforme a norma NBR ISO/IEC 17799, a segurança organizacional tem como objetivo a gerência da segurança da informação dentro da organização. Convêm que uma estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação na organização. Tendo como foco principal a proteção de pessoas, ativos, bens e instalações, garantindo a integridade e a continuidade do negócio.

A organização deve assegurar que as metas de segurança da informação estejam identificadas e que atendam aos requisitos da mesma fornecendo recursos necessários para segurança da informação.

Quadro 3 – Segurança organizacional.

Prática	Aderência		
	Sim	Sim, porém desatualizada	Não
Infraestrutura de segurança da informação para gerenciar as ações coorporativas?			X
Fórum de segurança formado pelo corpo diretor, a fim de gerir mudanças estratégicas?			X
Definição clara das atribuições de responsabilidade associadas à			X

segurança da informação?			
Identificação dos riscos no acesso de prestadores de serviço?		X	
Controle de acesso específico para os prestadores de serviço?	X		
Requisitos de segurança dos contratos de terceirização?			X

Fonte: do autor, 2015, teste de conformidade (Sêmola, 2003).

O Quadro 3 demonstra que a segurança organizacional inspira cuidados, pois a grande maioria das respostas é negativa a aderência totalizando três pontos de um total de doze possíveis. Demonstra também que um quesito está em conformidade e apenas um está parcialmente em conformidade com a norma.

Percebe-se que existe uma dificuldade do gestor em entender a importância da segurança organizacional na Prefeitura, pois requisitos básicos e fundamentais são descumpridos, dessa forma infringindo a legislação vigente.

5.1.3 Classificação e controle dos ativos

Todos os ativos devem ser inventariados e de responsabilidade de um proprietário para alcançar a proteção adequada na organização. Convém que o proprietário do ativo, já identificado, seja atribuído o controle e manutenção apropriada (NBR ISO/IEC 17799, 2005). Conforme a norma a delegação de controles específicos deverá ser realizada pelo proprietário dos ativos.

Os ativos devem ser identificados e documentados, classificados de acordo com os níveis de importância que necessitar e para isso deve ser definido um conjunto de medidas e tratamentos apropriados para essa classificação.

Quadro 4 – Classificação e controle dos ativos.

Prática	Aderência		
	Sim	Sim, porém desatualizada	Não
Inventário dos ativos físicos, lógicos e humanos?	X		
Critérios de classificação da informação?	X		

Fonte: do autor, 2015, teste de conformidade (Sêmola, 2003).

O Quando 4 demonstra a aderência à classificação e controle dos ativos na organização. Verifica-se que os quesitos estão aderentes a norma, pois a pontuação máxima foi atingida, evidenciando o interesse e a preocupação da organização em relação à classificação e controle dos ativos.

5.1.4 Segurança em pessoas

Para NBR ISO/IEC 17799/2005, segurança em pessoas objetiva assegurar que funcionários, fornecedores e terceiros estejam de acordo com seus papeis e cientes de suas responsabilidades, com intuito de minimizar os riscos de fraudes, roubos e má uso de recursos.

Deve ser realizada uma análise adequada antes de realizar uma contratação como também assegurar que a responsabilidade de segurança da informação seja definida e documentada de acordo com a política de segurança da informação da organização.

Quadro 5 – Segurança em pessoas.

Prática	Aderência		
	Sim	Sim, porém desatualizada	Não
Critérios de seleção e política de pessoal?	X		
Acordo de confidencialidade, termos e condições de trabalho?	X		
Processos para capacitação e treinamento de usuários?		X	
Estrutura para notificar e responder aos incidentes e falhas de segurança?	X		

Fonte: do autor, 2015, teste de conformidade (Sêmola, 2003).

Na avaliação do Quadro 5 que apresenta a aderência à segurança em pessoas, pode-se observar que a organização adota uma política criteriosa na seleção de pessoal, sendo ela mediante concurso público e licitação, os quais são contratados ao preencher requisitos preestabelecidos, o que evidencia o elevado grau de aderência à norma.

Existem normas de conduta que regulamentam a função pública. Dessa forma todos que atuam na função pública estão cientes de suas responsabilidades. Além disso, a Prefeitura possui uma comissão de sindicância nomeada pelo gestor que é responsável pela investigação e notificação dos responsáveis por eventuais incidentes.

Em relação ao quesito de capacitação e treinamento de usuários está parcialmente em conformidade com a norma, pois não ocorre frequentemente.

5.1.5 Segurança física e de ambiente

Conforme a norma NBR ISO/IEC 17799/2005, a segurança física e do ambiente objetiva prevenir o acesso físico não autorizado, danos e interferência com as informações e instalações da organização. Devendo as instalações e informações ser mantidas em áreas seguras, protegidas por barreiras de segurança e controles de acessos apropriados.

Quadro 6 – Segurança física e de ambiente.

Prática	Aderência		
	Sim	Sim, porém desatualizada.	Não
Definição de perímetros e controles de acesso físico aos ambientes?			X
Recursos para segurança e manutenção dos equipamentos?		X	
Estrutura para fornecimento adequado de energia?			X
Segurança do cabeamento?			X

Fonte: do autor, 2015, teste de conformidade (Sêmola, 2003).

O Quadro 6 demonstra que a segurança física e de ambiente nesta organização não está aderente à norma, pois num total de dezesseis pontos a

organização atingiu um único ponto, o que demonstra um desconhecimento ou desinteresse pela segurança física e de ambiente.

Com essa avaliação foi constatado que não existem controles de perímetros e de acesso físico aos ambientes, tão pouco a estrutura física de um CPD (Data Center). O servidor está alocado na sala da tesouraria não envolvendo critérios de segurança. Sequer a porta é trancada, possibilitando o livre acesso a qualquer pessoa.

O fornecimento adequado de energia também é preocupante. A fiação, plugues e tomadas são antigas em desacordo com a ABNT NBR 14136:2002. Na falta de energia, tudo para de funcionar, pois não há nenhum gerador de energia complementar. Somente o servidor possui um *nobreak* que tem uma autonomia de até 2 horas. Normas que dizem respeito ao cabeamento também não são observadas, fato que é evidenciado pela inexistência de aterramento da rede elétrica e pela inexistência de uma estrutura padronizada de cabeamento lógico.

5.1.6 Gerenciamento das operações e comunicações

O gerenciamento das operações e comunicações conforme a norma NBR ISO/IEC 17799 tem como objetivo a operação correta e segura dos recursos de processamento da informação. Como também o desenvolvimento de procedimentos operacionais apropriados através da definição de processos.

Quadro 7 – Gerenciamento das operações e comunicações.

Prática	Aderência		
	Sim	Sim, porém desatualizada.	Não
Procedimentos e responsabilidades operacionais?		X	
Controle de mudanças operacionais?			X
Segregação de funções e ambientes?		X	
Planejamento e aceitação de sistemas?		X	
Procedimentos para cópias de segurança?	X		

Controles e gerenciamento de rede?	X		
Mecanismos de segurança e tratamento de mídias?		X	
Procedimentos para documentação de sistemas?	X		
Mecanismos de segurança do correio eletrônico?			X

Fonte: do autor, 2015, teste de conformidade (Sêmola, 2003).

O Quadro 7 apresenta a aderência do gerenciamento das operações e comunicações da Prefeitura. Percebe-se que, dos nove quesitos deste quadro, quatro são parcialmente aderentes e dois não são aderentes à norma.

A não aderência ao quesito de mecanismos de segurança do correio eletrônico é preocupante, pois isso demonstra que a organização não realiza um controle efetivo sobre ele, tornando assim a segurança da informação vulnerável.

Verifica-se que três quesitos de gerenciamento das operações e comunicações são aderentes à norma, entre eles os procedimentos para cópias de segurança, os quais a organização tem o cuidado de realizar Backup duas vezes ao dia. Outro quesito relevante é o controle e gerenciamento de rede. Para isso a organização instalou um software que controla e gerencia a rede interna, restringindo o acesso a sites específicos.

5.1.7 Controle de acesso

O objetivo da norma NBR ISO/IEC 17799/2005, é assegurar o acesso de usuários autorizados e prevenir acessos não autorizados a sistemas de informação. Procedimentos formais devem ser implementados para gerenciar e controlar a distribuição de direitos de acesso a sistemas informatizados e serviços.

Esses procedimentos devem ocorrer desde a liberação de acesso até o cancelamento do acesso. Outro cuidado deve ser tomado com os privilégios que cada usuário possui.

Quadro 8 – Controle de acesso.

Prática	Aderência		
	Sim	Sim, porém desatualizada.	Não
Requisitos do negócio para controle de acesso?	X		
Gerenciamento de acesso do usuário?		X	
Controle de acesso à rede?		X	
Controle de acesso ao sistema operacional?	X		
Controle de acesso às aplicações?	X		
Monitoração de uso e acesso ao sistema?	X		
Critérios para computação móvel e trabalho remoto?		X	

Fonte: do autor, 2015, teste de conformidade (Sêmola, 2003).

O Quadro 8 demonstra a aderência ao controle de acesso à norma e nota-se que a Prefeitura Municipal tem uma aderência considerável, pois soma onze pontos de catorze pontos possíveis.

Em relação aos acessos a sistemas, cada usuário possui um *login* e senha com permissão de operar apenas o módulo destinado, existindo um monitoramento que permite a identificação do usuário.

Constata-se que três quesitos de controle de acesso são parcialmente aderentes à norma, sendo fundamental uma maior atenção da organização a esses quesitos.

5.1.8 Desenvolvimento e manutenção de sistemas

Conforme norma NBR ISO/IEC 17799/2005, o desenvolvimento e manutenção de sistemas servem para garantir que a segurança seja parte integrada dos sistemas de informação.

Para isso todos os requisitos de segurança devem ser identificados e justificados na fase de levantamento de requisitos de um projeto, acordados e documentados como parte geral do caso de um negócio para um sistema de informação.

Quadro 9 – Desenvolvimento e manutenção de sistemas.

Prática	Aderência		
	Sim	Sim, porém desatualizada.	Não
Requisitos de segurança de sistemas?		X	
Controle de criptografia?	X		
Mecanismos de segurança nos processos de desenvolvimento e suporte?		X	

Fonte: do autor, 2015, teste de conformidade (Sêmola, 2003).

No Quadro 9 apresenta-se a aderência da organização ao desenvolvimento e manutenção de sistemas e evidencia-se que está aderente ao controle de criptografia. A Prefeitura Municipal faz uso da criptografia através da identidade digital. Essa que é obrigatória para alguns funcionários poderem acessar sites específicos. Os sites mais comuns são os governamentais e do setor bancário, pois a grande parte dos pagamentos, transferências e depósitos são de modo on-line.

Em relação aos Requisitos de segurança de sistemas e Mecanismos de segurança nos processos de desenvolvimento e suporte, a Prefeitura Municipal está parcialmente aderente à norma, o que remete uma maior atenção aos mesmos.

5.1.9 Gestão de incidentes de segurança da informação.

O objetivo da gestão de incidentes de segurança da informação é assegurar que fragilidades e eventos de segurança da informação, associados com sistemas de informação sejam comunicados em tempo hábil para eventuais ações corretivas (NBR ISO/IEC 17799, 2005).

Quadro 10 – Gestão de incidentes da segurança da informação.

Prática	Aderência		
	Sim	Sim, porém desatualizada.	Não
Existe um processo formalizado e implantado para o tratamento dos incidentes?			X
Existe uma estrutura responsável pelo tratamento dos incidentes?			X

Fonte: do autor, 2015, teste de conformidade (Sêmola, 2003).

Em análise ao Quadro 10, percebe-se que a Prefeitura Municipal não está aderente aos quesitos da Gestão de incidentes da segurança da informação, pois não possui nenhum processo formalizado, como também não há uma estrutura responsável pelo tratamento de incidentes. Esse quesito torna-se, portanto, um ponto crítico na segurança da informação da organização.

Conforme a norma, procedimentos formais devem ser estabelecidos e de conhecimento dos funcionários, terceiros e fornecedores sendo notificados tão logo quanto possível.

5.1.10 Conformidade

Para norma NBR ISO/IEC 17799 a conformidade deve evitar violações de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais e de requisitos de segurança da informação. Convém que todos os requisitos estatutários, regulamentares e contratuais sejam definidos, documentados e mantidos atualizados para cada sistema de informação.

Quadro 11 – Conformidade

Prática	Aderência		
	Sim	Sim, porém desatualizada.	Não
Gestão de conformidade técnicas e legais?		X	
Recursos e critérios para auditoria de sistemas?			X

Fonte: do autor, 2015, teste de conformidade (Sêmola, 2003).

O Quadro 11 apresenta a aderência à conformidade ou não da Prefeitura Municipal. Com o levantamento realizado, percebe-se que a mesma não está aderente em relação a recursos e critérios para auditoria de sistemas. Já em relação à gestão de conformidades técnicas e legais está parcialmente aderente à norma.

No momento, a Prefeitura Municipal não conta com funcionário que seja responsável por auditorias de sistemas dificultando ainda mais a aderência à conformidade.

5.2 Índices de conformidade com a norma ISO/IEC 17799

Os valores apresentados abaixo servirão como base de definição do grau de aderência da Prefeitura em relação norma NBR ISO/IEC 17799.

a) Resultado entre 80 – 54

Para Sêmola (2003) se os resultados forem entre 80 – 54, a organização está de parabéns, por conta da abrangência dos controles que aplica no negócio e da conscientização pela importância da segurança. Dessa maneira a empresa é uma exceção e deve estar em destaque.

b) Resultado entre 53 – 27

Esse resultado requer atenção, a empresa pode ter adotados todos os quesitos, mas pode estar desatualizada ou inativa, o que demonstra um bom nível de consciência, e também de deficiência na estrutura de gestão. Poderia ser a falta de recursos financeiros para subsidiar os recursos da administração.

c) Resultado entre 26 – 0

Essa situação não é confortável quando os resultados forem entre 26 – 0 é preciso tomar cuidado. A segurança da informação não está sendo tratada como prioridade, indicando a ausência ou ineficácia de muitos dos controles recomendados. A causa pode ser o desconhecimento dos riscos e a falta de sensibilização dos gestores da alta administração.

Tabela 1 - Teste de conformidade, pontuação obtida na Prefeitura Municipal

Respostas	Pontuação
Resposta A	14 – 28 pontos
Resposta B	13 – 13 pontos
Resposta C	13 – 0 pontos
	Total: 41 pontos

Fonte: do autor, 2015 baseado em dados da organização.

Na Tabela 1 apresenta-se o resultado da soma de pontos obtidos na pesquisa realizada, considerando a pontuação do Quadro 1.

Tabela 2 - Avaliação do grau de aderência

Domínio	Pontuação Máxima	Pontos Obtidos	Grau de aderência
Política de segurança	4	0	0%
Segurança organizacional	12	3	25%
Classificação e controle dos ativos de informação	4	4	100%
Segurança em pessoas	8	7	87%
Segurança física e de ambiente	8	1	12%
Gerenciamento das operações e comunicações	18	10	56%
Controle de acesso	14	11	79%
Desenvolvimento e manutenção de sistemas	6	4	67%
Gestão de incidentes da segurança da informação	4	0	0%
Conformidade	4	1	25%
Total		**41**	**51% (média)**

Fonte: do autor 2015, baseado em dados da organização.

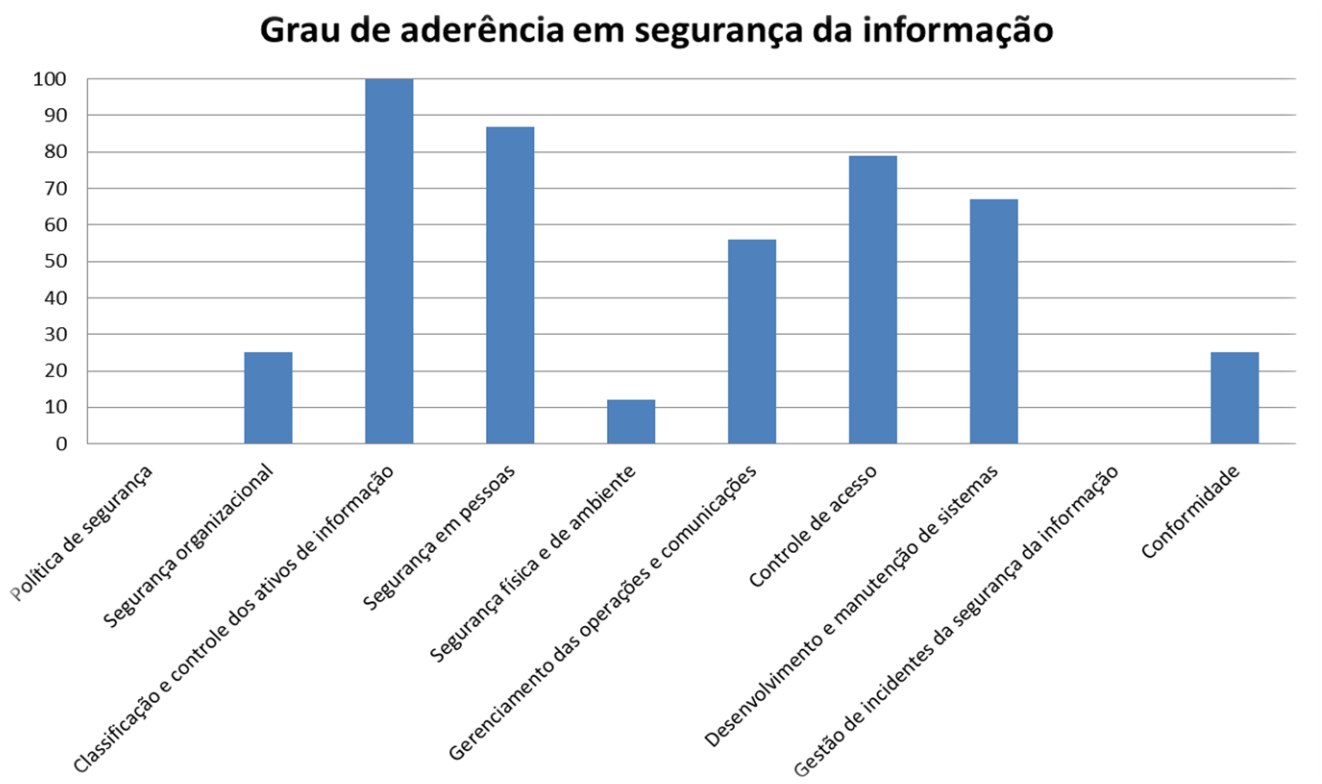
Com base na tabela 2, pode-se verificar que a Prefeitura Municipal de Travesseiro atingiu 41 pontos de um total de 80 pontos possíveis, indicando que a organização atua com 51% de aderência à norma NBR ISO/IEC 17799.

O resultado de 41 pontos está entre 53 – 27 que, conforme Sêmola (2003) requer atenção. A Prefeitura Municipal pode ter adotado todos os quesitos, mas estes podem estar desatualizados, inativos ou não divulgados, que demonstra, por um lado, um bom nível de consciência e, por outro, podendo também demonstrar certa deficiência na estrutura de gestão da segurança em TI.

Esse resultado demonstra ainda que os processos relacionados com a segurança da Tecnologia da Informação requerem atenção por parte dos gestores e especialistas em segurança desta organização.

O gráfico 1, a seguir, demonstra os índices apresentados na tabela 2.

Gráfico 1 – Índices do grau de aderência à norma NBR ISO\IEC 17799.



Fonte: autor 2015, dados da organização.

Considerando a Tabela 2, verifica-se que a aderência é 0% nos quesitos de Política de segurança e Gestão de incidentes da segurança da informação. Evidencia que a situação da Prefeitura em relação a esses quesitos não é confortável e é preciso ter cuidado. A organização deve tomar algumas medidas urgentes para reverter a atual situação.

O mesmo pode-se dizer para os quesitos de Segurança física, Segurança organizacional e Conformidade, pois os índices de aderência variam de 12% a 25%, demonstrando que a Prefeitura Municipal não trata a segurança como prioridade.

Por outro lado, o gerenciamento das operações e comunicações apresenta um índice de 56% de aderência à norma. Pode-se dizer que a Prefeitura Municipal está adotando parte dos quesitos ou até todos eles, mas, desatualizados, evidenciando que a segurança da informação requer atenção.

Os quesitos de Desenvolvimento e manutenção de sistemas com 67%, Controle de acesso com 79%, Segurança de pessoas com 87% e Classificação e controle dos ativos de informação com 100% de aderência, demonstram que a Prefeitura Municipal está consciente da importância destes itens na segurança da informação, aplicando-os e divulgando-os.

5.3 Análise da Lei 12.527/2011 – Acesso à Informação

O objetivo é verificar a aderência da Prefeitura Municipal de Travesseiro à Lei 12.527/2011 – Lei de Acesso à Informação.

Como não foi identificado nenhum método específico para essa abordagem, utiliza-se os mesmos critérios que Sêmola (2003) utilizou para estabelecer o grau de aderência à norma NBR ISO/IEC 17799. Para isso é necessário ajustar os valores da tabela assim como os valores dos limites de classificação. Na abordagem inicial (Grau de aderência à norma ISO\IEC 17799), o autor chega a um valor máximo de 80 pontos. Já na avaliação do grau de aderência à Lei de Acesso à Informação a pontuação chega a um valor máximo de 288 pontos. Esses pontos são alcançados mediante a multiplicação do número de respondentes (8 respondentes) pelo total possível de respostas “Sim” (dezoito quesitos), que valem individualmente dois pontos.

O diagnóstico é simples e rápido baseado em perguntas objetivas, realizadas aos funcionários responsáveis pelo setor em que trabalham. Com uma pontuação baseada no grau de aderência à segurança da informação de Sêmola (2003), que irá revelar seu índice de aderência à lei.

O Quadro 12 mostra a tabela de pontuação utilizada para avaliar o grau de aderência obtido, com os resultados da pesquisa aplicada na Prefeitura Municipal, tendo cada resposta uma pontuação própria.

Quadro 12 – Lei de acesso à informação: Tabela de pontuação

Resposta A: (Sim) some 2 pontos. Resposta B: (Sim, em parte) some 1 ponto. Resposta C: (Não) não some, nem subtraia pontos.

Fonte: Do autor, 2015.

5.3.1 Princípio da legalidade

O princípio da legalidade, embora não esteja presente na lei é incluído no presente trabalho com o objetivo de verificar o conhecimento e prática da lei na Prefeitura Municipal.

Quadro 13 – Princípio da legalidade

Questão	Resposta		
	Sim	Sim, em parte.	Não
Você tem conhecimento da Lei 12.527/2011 que garante o Acesso a Informação para a população?	3	5	
A Lei de Acesso a Informação é aplicada no setor em que você trabalha?	5	3	
Existe regulamentação própria definindo regras especificas visando a segurança da informação?			8
Foi realizado treinamento sobre a Lei de Acesso a Informação?	2		6
As informações geradas no setor são auditadas?	4	3	1

Fonte: autor, 2015.

De um total de 80 pontos possíveis a análise do princípio da legalidade apresenta 42 pontos.

Com base no Quadro 13 fica evidente que a Lei de Acesso à Informação não está sendo aplicada em todos os setores da Prefeitura Municipal. Mesmo estando em vigor desde maio de 2012 e obrigatória para municípios com menos de 50 mil habitantes a partir de maio de 2013, alguns itens da lei são descumpridos.

Mesmo que o conhecimento da lei seja obrigatório, apenas três funcionários tem o conhecimento total e os outros cinco têm conhecimento de parte desta lei.

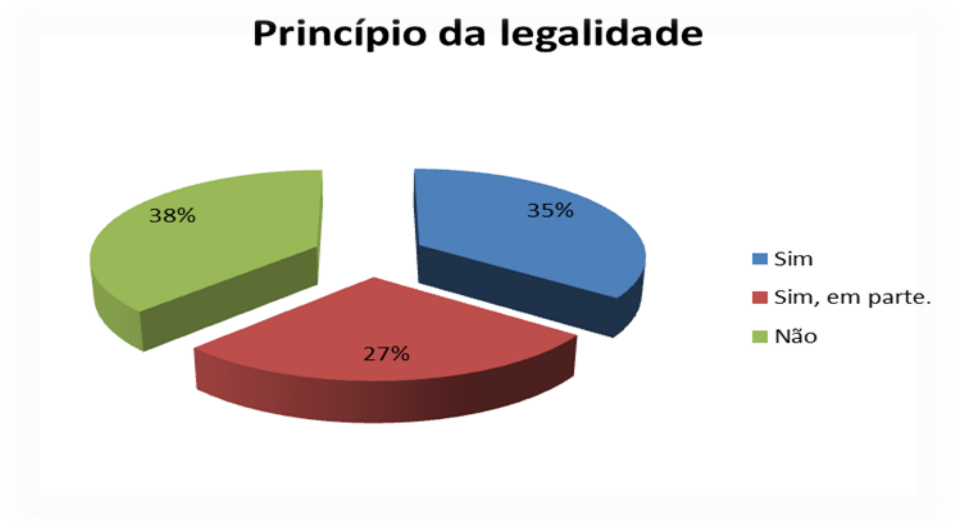
Atualmente a Lei de Acesso a Informação não está sendo aplicada em todos os setores, demonstrando que esses setores estão em desacordo com a Lei de Acesso à Informação, podendo assim, os responsáveis pelas informações serem notificados e penalizados pelo descumprimento da lei.

O quesito que diz respeito à regulamentação própria demonstra que não há aderência à Lei de Acesso à Informação, embora a Prefeitura Municipal seja obrigada a regulamentar com leis próprias a segurança da informação.

Quanto ao item de treinamento, somente duas pessoas o realizaram, demonstrando certa desconsideração em relação à Lei de Acesso à Informação.

Percebe-se que o item que apresenta o quesito de auditoria, totalizou onze pontos de dezesseis pontos possíveis. Isso demonstra uma boa aderência da Prefeitura Municipal à Lei de Acesso à Informação.

Gráfico 2 – Princípio da Legalidade.



Fonte: Do autor, 2015.

O gráfico 2 que representa os quesitos do princípio da legalidade percebe-se que apenas 35% dos itens são realizados conforme a lei determina, já 27% deles são realizados em parte e 38% não são realizados, desta forma descumprindo completamente a Lei.

5.3.2 Classificação da informação

Conforme a Lei de Acesso à Informação, a informação em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, poderá ser classificada como ultrassecreta, secreta ou reservada.

Tendo prazos máximos de restrição, conforme a classificação prevista em lei, sendo de vinte e cinco (25) anos para informações ultrassecretas, quinze (15) anos para informações secretas e cinco (5) anos para informações reservadas. Os prazos vigoram a partir da data de sua produção.

Independentemente de classificação de sigilo, as informações pessoais que diz respeito à intimidade, vida privada, honra e imagem da pessoa, não podem ser divulgadas pelo prazo máximo de 100 anos a contar da sua data de produção. Mas, poderão ser divulgadas por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referem.

Quadro 14 – Classificação da informação

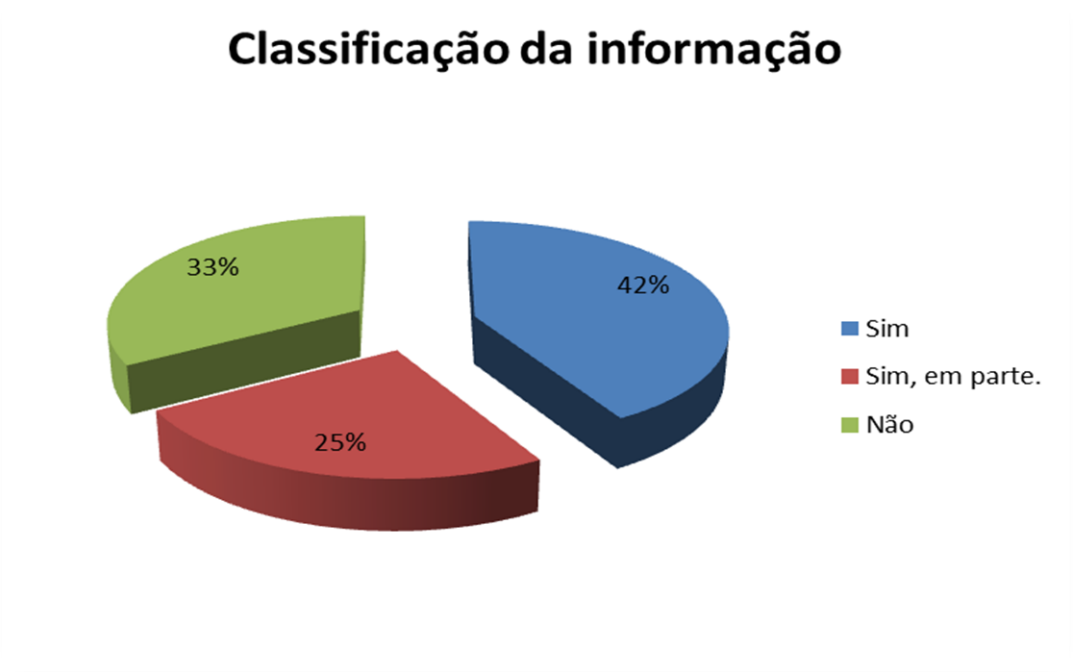
Questão	Resposta		
	Sim	Sim, em parte	Não
As informações geradas no setor estão de acordo com o sigilo exigido pela lei?	1	2	5
As informações de cunho pessoal são tratadas de acordo com a Lei?	7	1	
São conhecidos os prazos de cada classificação?	2	3	3

Fonte: autor, 2015.

O Quadro 14 apresenta a aderência à classificação da informação na Prefeitura Municipal, demonstrando que, de 48 pontos possíveis, somou-se 26 pontos.

O quesito com mais aderência à lei trata sobre as informações de cunho pessoal totalizando 15 pontos de 16 pontos possíveis, demonstrando que é dado uma maior importância, pois o seu descumprimento pode implicar em penalidades civis.

Gráfico 3 – Classificação da informação.



Fonte: Do autor, 2015.

Os quesitos de classificação da informação, são representados pelo Gráfico 3, que demonstra a aderência à lei pelos setores da Prefeitura Municipal é de 42%. A aderência parcial representa 25% e os que não aderiram à lei representa 33%.

5.3.3 Tratamento da informação

A Lei de Acesso à Informação prevê que todos os órgãos e entidades públicas são obrigados a divulgar em sítios oficiais da rede mundial de computadores as informações de interesse público.

As informações disponíveis para acesso devem ser atualizadas, autênticas, íntegras e possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações.

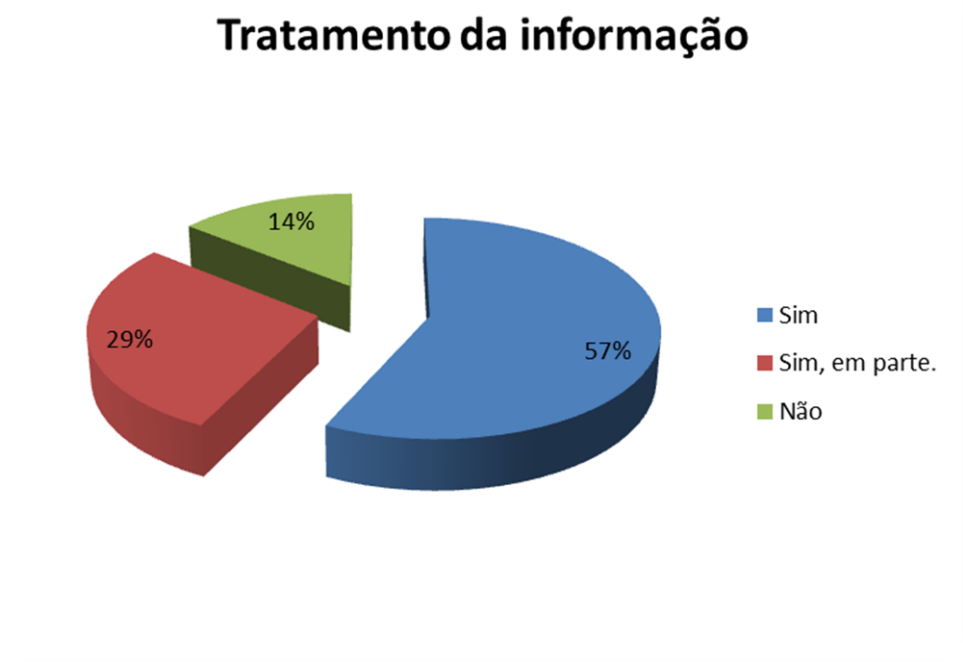
Quadro 15 – Tratamento da informação

Questão	Resposta		
	Sim	Sim, em parte	Não
As informações são disponibilizadas em sítios oficiais?	3	4	1
As informações disponibilizadas nos sítios oficiais são de formato padronizado?	4	2	2
As informações disponibilizadas nos sítios oficiais são seguras?	7		1
As atualizações das informações nos sítios oficiais são constantes?	2	2	4

Fonte: autor, 2015.

O Quadro 15 demonstra que o quesito com melhor aderência à Lei, é o da segurança na disponibilidade das informações nos sítios oficiais, o qual totalizou 14 pontos de 16 pontos possíveis, evidenciando a preocupação com a segurança da informação.

Gráfico 4 – Tratamento da informação.



Fonte: Do autor, 2015.

O Gráfico 4 demonstra que 57% dos entrevistados responderam que “sim”. Esses estão aderentes à Lei. Já 29% estão parcialmente aderentes e 14% não estão aderentes à Lei, evidenciando, que está sendo infringido o Art. 8º da Lei de Acesso à Informação, que diz:

> É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas (BRASIL, 2011).

5.3.4 Garantia de acesso

Conforme a Lei de Acesso a Informação é dever de o órgão público garantir o acesso à informação. Essa informação deve ser de qualidade obedecendo aos princípios da disponibilidade, autenticidade, integridade e da primariedade.

Quadro 16 – Garantia de acesso

Questão	Resposta		
	Sim	Sim, em parte	Não
As informações geradas no seu setor obedecem aos princípios da disponibilidade?	8		
As informações geradas no seu setor obedecem aos princípios da autenticidade?	7	1	
As informações geradas no seu setor obedecem aos princípios da integridade?	8		
As informações geradas no seu setor obedecem aos princípios da primariedade?	6	1	1

Fonte: Do autor, 2015.

O Quadro 16 apresenta a garantia de acesso às informações na Prefeitura Municipal, de um total de 64 pontos possíveis, alcançou-se 60 pontos.

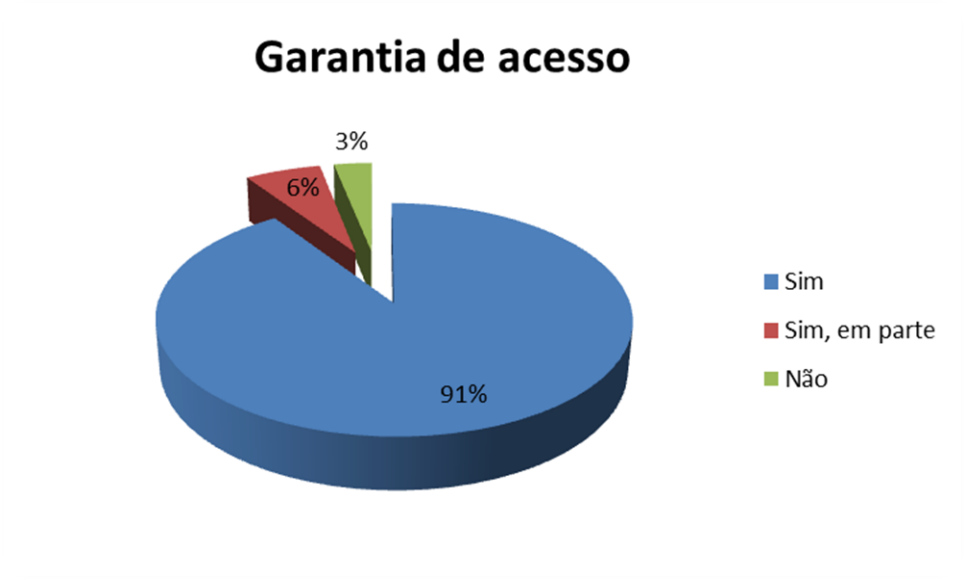
Conforme a lei, a disponibilidade é a qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados, sendo esse princípio obedecido por todos os entrevistados.

A qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema, pertence ao princípio da autenticidade, sendo que dos oito entrevistados, sete cumprem esse princípio e um cumpre parcialmente.

Já a integridade é elencada como um dos principais quesitos. Atualmente ela está sendo cumprida por todos os setores. Isso garante que a qualidade da informação não está sendo modificada inclusive quanto à origem, trânsito e destino.

Em relação aos princípios da primariedade que diz a respeito à qualidade da informação coletada na fonte com o máximo de detalhamento possível sem modificações, deve haver um cuidado, pois, um dos setores pesquisados não está aderente com a lei e outro setor segue em parte esse quesito.

Gráfico 5 – Garantia de acesso.



Fonte: Do autor, 2015.

No gráfico 5 que apresenta os quesitos da Garantia de acesso, percebe-se que 3% das respostas foram “não”, já 6% responderam em parte e 91% responderam que “sim”, demonstrando que o resultado da aderência à Lei de Acesso à Informação é satisfatório.

5.3.5 Condutas e responsabilidades

Os órgãos e entidades públicas, conforme a lei, respondem diretamente pelos danos causados em decorrência da utilização indevida de informações, cabendo à apuração de responsabilidade funcional nos casos de dolo ou culpa.

A responsabilidade é aplicada à pessoa física ou entidade privada com vínculo de qualquer natureza com órgãos ou entidades públicas, sujeito a advertência, multa, rescisão de vínculo, suspensão temporária de participar de licitação e declaração de inidoneidade para licitar ou contratar com a administração pública.

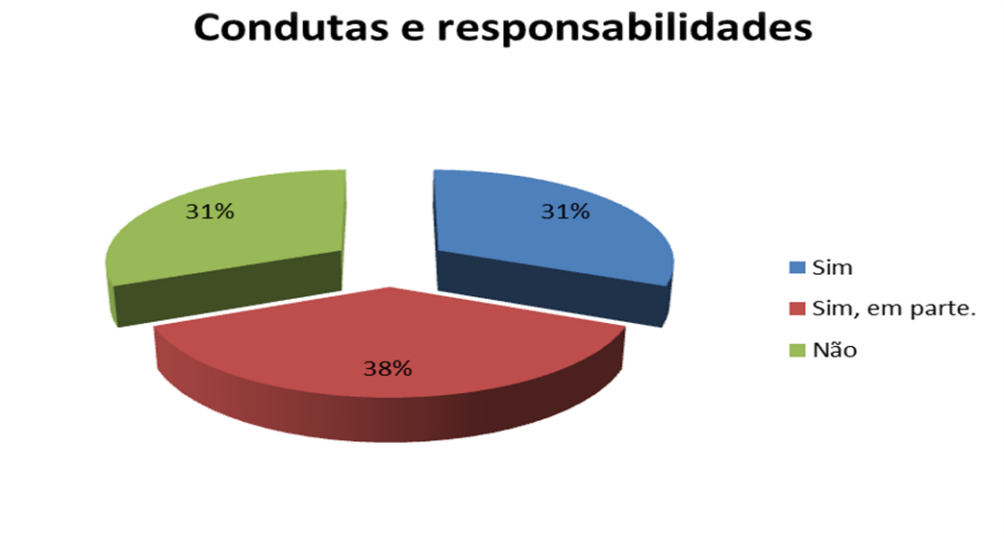
Quadro 17 – Condutas e responsabilidades

Questão	Resposta		
	Sim	Sim, em parte	Não
Você sabe das obrigações sobre a guarda de sigilo?	3	1	4
Você sabe das responsabilidades sofridas pelo agente público, por conduta ilícita com as informações?	2	5	1

Fonte: Do autor, 2015.

O Quadro 17 apresenta as condutas e responsabilidades da Prefeitura Municipal em relação à lei. Percebe-se que não existe uma aderência satisfatória, sendo que de 32 pontos possíveis, totalizou-se 16 pontos.

Gráfico 6 – Condutas e responsabilidades.



Fonte: Do autor, 2015.

O Gráfico 6 demonstra que 31% dos respondentes conhecem as condutas e responsabilidades conforme a lei. Já 38% conhecem parcialmente e 31% não conhecem as condutas e responsabilidades. No entanto, a falta de conhecimento da lei não isenta o responsável de sofrer punições.

5.4 Percepção dos entrevistados quanto a Prefeitura Municipal de Travesseiro

O Quadro 18 apresenta a percepção dos usuários em relação à Prefeitura Municipal de Travesseiro. Essa análise não está diretamente direcionada à Lei de Acesso a Informação e não há um alinhamento das respostas relacionadas com o Quadro 19.

A pontuação gerada não faz parte da pontuação geral sobre o grau de aderência à norma NBR ISO/IEC 17799 e nem da pontuação de aderência à Lei de Acesso à Informação.

O quadro abaixo apresenta as respostas obtidas com o questionário aplicado aos funcionários da Prefeitura Municipal.

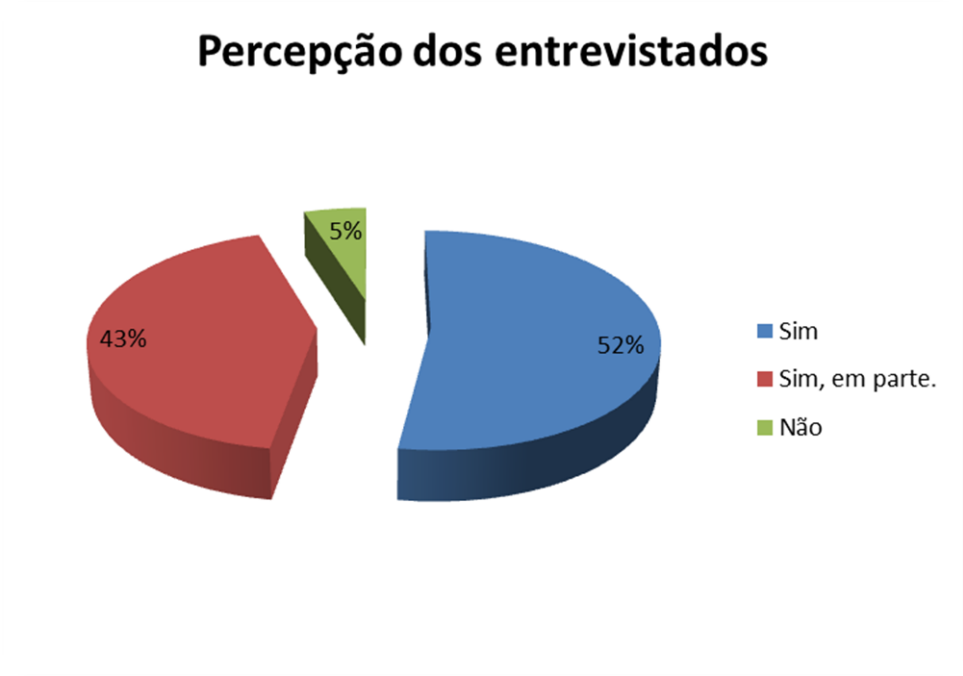
Quadro 18 – Percepção dos entrevistados quanto a Prefeitura Municipal de Travesseiro

Questão	Resposta		
	Sim	Sim, em parte	Não
O acesso à informação da Prefeitura Municipal de Travesseiro está de acordo com a Lei e com as boas práticas de Tecnologia da Informação?	3	5	
A disponibilização das informações está obedecendo ao formato padronizado?	3	4	1
A guarda das informações é segura?	6	1	1
O site no qual as informações são disponibilizadas é seguro?	6	2	
A Prefeitura Municipal de Travesseiro está de acordo com as boas práticas de segurança da informação?	3	5	

Fonte: Do autor, 2015.

Os quesitos nos quais a Prefeitura Municipal obteve melhor avaliação são aqueles que se referem à guarda das informações com segurança e à disponibilização segura no site. Em ambos, seis respondentes de um total de oito responderam ”sim”. Assim, segundo eles, há uma boa segurança em relação a esses quesitos.

Gráfico 7 – Percepção dos entrevistados



Fonte: Do autor, 2015.

O Gráfico 7 demonstra que para 52% dos entrevistados que responderam “sim” a Prefeitura Municipal de Travesseiro está de acordo com a Lei de Acesso à Informação e também está seguindo as boas práticas de segurança da informação. Para 6% dos entrevistados a Prefeitura Municipal não está de acordo, desse modo descumprindo a Lei de Acesso à Informação e as boas práticas de segurança da informação. Já para 43% dos entrevistados as boas práticas de segurança da informação e a Lei de Acesso à Informação estão sendo cumpridas parcialmente.

A Tabela 3 apresenta a soma dos pontos obtidos na pesquisa realizada, de acordo com a pontuação estabelecida no Quadro 12.

Tabela 3 – Grau de aderência à Lei de Acesso à Informação

Respostas	Pontuação
Resposta A – Sim	74 – 148 pontos
Resposta B – Sim em parte	33 – 33 pontos
Resposta C – Não	33 – 0 pontos
	Total: 181 pontos

Fonte: do autor 2015, baseado em dados da organização.

A Tabela 3 foi criada com a base na Tabela de Teste de Conformidade de Sêmola (2003), sendo cada resposta “SIM” = 2 pontos, “SIM, EM PARTE” = 1 ponto e “NÃO” = 0 ponto, somando assim todos os pontos, obteve-se um resultado de 181 pontos.

No entanto, os 288 pontos que equivalem a 100% de aderência à Lei de Acesso a Informação, correspondem aos 80 pontos obtidos em 100% de aderência à norma NBR ISO/IEC 17799, nessa comparação chega-se à conclusão que 288 é 3,6 vezes maior que 80.

Com isso pode-se dizer que os valores entre 26 – 0, 53 – 27 e 80 – 54 criados por Sêmola equivalem respectivamente a 96 – 0, 192 – 96 e 288 – 193 utilizados para avaliar o grau de aderência à Lei de Acesso à Informação. Sendo assim, poderemos comparar as duas pesquisas, pois elas se utilizam dos mesmos critérios de pontuação e porcentagem.

Tabela 4 – Avaliação do grau de aderência

Item	**Pontuação Máxima**	**Nº de Pontos**	**Aderência a LAI**
Princípio da Legalidade	80	39	48%
Classificação da informação	48	26	54%
Tratamento da informação	64	40	62%
Garantia de acesso	64	60	93%
Condutas e Responsabilidades	32	16	50%
Total	**288 Pontos**	**181 Pontos**	**62% (média)**

Fonte: do autor 2015, baseado em dados da organização.

Percebe-se que todos os quesitos apresentados na Tabela 4, demonstram que a aderência à Lei de Acesso à Informação na Prefeitura Municipal de Travesseiro requer atenção. Por se tratar de uma lei, pode-se dizer que ela está sendo cumprida parcialmente, sendo que deveria ser cumprida por total.

Na avaliação geral de aderência à Lei de Acesso à Informação da Prefeitura Municipal, chega-se a uma aderência média de 62%.

5.5 Alinhamento da Lei de Acesso à Informação e Norma NBR ISO/IEC 17799

No Quadro 19 será apresentada uma análise de alinhamento entre os resultados da aderência à Lei de Acesso à Informação em relação aos resultados de aderência à norma ISO/IEC 17799.

Quadro 19 – A aplicação da norma em relação à Lei de Acesso à Informação

Lei de Acesso a Informação	Percentual atingido	Norma ISO/IEC 17799	Percentual médio	Alinhado?
Princípio da Legalidade	48%	Conformidade Política de segurança da informação Segurança em pessoas	37%	Não
Classificação da informação	54%	Desenvolvimento e manutenção de sistemas Controle de acesso Classificação e controle dos ativos	82%	Não
Tratamento da informação	62%	Gerenciamento das operações e comunicações	56%	Sim
Garantia de acesso	93%	Gerenciamento das operações e comunicações Desenvolvimento e manutenção de sistemas Segurança física e de ambiente	45%	Não
Condutas e Responsabilidades	50%	Gestão de incidentes da segurança da informação Segurança organizacional	12%	Não

Fonte: Do autor, 2015.

A análise entre os diferentes resultados é feita a partir da utilização dos valores referentes à Lei de Acesso a Informação como base na comparação com a norma NBR ISO/IEC 17799, que está apresentada no Quadro 19.

Para o item *Princípio da legalidade* o valor médio do grau de aderência à Lei de Acesso à Informação é de 48% enquanto que a média no bloco relacionado a esse item da aderência à norma é de 37%. Pelo fato desses valores terem ficado abaixo de 60% aponta-se que deverá haver uma maior atenção da Administração Municipal sobre os quesitos apresentados.

O item *Classificação da informação* apresenta uma média do grau de aderência à Lei de Acesso à Informação de 54%, e a média alcançada na norma foi de 82%, demonstrando que não há um alinhamento entre a lei e a norma. Os percentuais de aderência à norma são bons, já os percentuais de aderência à lei requerem atenção.

O *Tratamento da informação* representa uma aderência de 62% à Lei de Acesso à Informação e uma média de 56% de aderência à norma. O item está alinhado, no entanto, também requer atenção, pois ainda não pode-se considerar que o nível de aderência apresentado seja o adequado.

Em relação à *Garantia de acesso*, o percentual atingido de aderência em relação à Lei e Acesso é de 93% enquanto a média em relação à norma é de 45% caracterizando um não alinhamento, mas verifica-se uma considerável aderência à Lei.

No que tange às *Condutas e Responsabilidades*, foi atingido um percentual de 50% de aderência à Lei de acesso à informação e uma média de 12% de aderência à norma. Verifica-se um não alinhamento e, além disso, a aderência à Lei requer uma maior atenção enquanto a aderência à norma apresenta um percentual crítico.

6 CONSIDERAÇÕES FINAIS

Com o presente estudo, foi possível efetuar um diagnóstico da situação da Prefeitura Municipal de Travesseiro na sua gestão de segurança na área da TI. Buscou-se conhecer melhor, em observância à norma ABNT NBR ISO/IEC 17799 e à Lei 12.527/2011 – Lei de Acesso à Informação, a aderência às mesmas, baseado em metodologias que abordassem os princípios da segurança da informação e de legislação. A norma NBR ISO/IEC 17799 que apresenta boas práticas de segurança de informação não é obrigatória quanto a sua implantação. Já a Lei de Acesso à Informação é obrigatória. Portanto deve ser cumprida totalmente.

De acordo com a análise sobre a aderência da Prefeitura Municipal de Travesseiro à norma ABNT NBR ISO/IEC 17799, constatou-se uma aderência de 51%, significando que a segurança da informação da Prefeitura requer atenção. Alguns requisitos de segurança são inexistentes, outros estão sendo seguidos, mas encontram-se desatualizados e inativos. Concluiu-se assim, que a falta de conhecimento por parte do gestor resultou nessa situação.

Com base na avaliação de aderência à norma, encontra-se em estado crítico a Política de Segurança da Informação e a Gestão de Incidentes da Segurança da Informação, pois os mesmos são inexistentes na organização.

A Segurança Física e de Ambiente, é um fator preocupante, pois não existe uma restrição e controle de acesso físico aos ambientes, possibilitando o livre acesso a qualquer pessoa à infraestrutura de informática, como também a

inexistência de um CPD (Data Center). A estrutura de fornecimento de energia está defasada, pois a rede elétrica é antiga e está em desacordo com as normas técnicas vigentes, sem plano de reposição de energia em caso de falta. Não existe a padronização do cabeamento lógico, o que pode ocasionar falhas na rede interna.

A situação da Segurança Organizacional e a Conformidade também preocupam, pois não existe um gerenciamento por parte do gestor para assegurar que as metas estabelecidas sejam cumpridas. Percebe-se a falta de auditoria e uma atualização quanto à regulamentação de requisitos de segurança da informação.

Por outro lado, a Classificação e Controle dos Ativos de Informação, Segurança em Pessoas, Controle de Acesso, Desenvolvimento e Manutenção de Sistemas estão sendo aplicados e existe uma preocupação em função da importância dos mesmos à organização, sendo que o nível em que se encontram é bom.

Constatou-se com a análise de aderência à Lei de Acesso a Informação que a Prefeitura Municipal de Travesseiro está com 62% de aderência, mesmo com o aumento de prazos de implantação concedidos pelo Governo Federal. Isso demonstra o desconhecimento da lei, pois está sendo cumprida parcialmente e vários itens estão sendo infringidos, o que pode acarretar em penalidades ao gestor e também ao responsável pela infração. Com isso, poderá a Prefeitura Municipal sofrer apontamentos dos órgãos de fiscalização como: Controle Interno, Tribunal de Contas do Estado (TCE) e Controladoria Geral da União (CGU).

No dia 15 de maio de 2015 a CGU divulgou em seu site e na imprensa nacional os resultados da pesquisa denominada “Escala Brasil Transparente”, que tem o objetivo de avaliar o grau de cumprimento de dispositivos da Lei de Acesso à Informação para aprofundar o monitoramento da transparência pública e gerar um produto que possibilite o acompanhamento das ações empreendidas por estados e municípios. A Prefeitura Municipal de Travesseiro foi um dos 492 municípios pesquisados, obtendo uma nota de 1,94 pontos de 0 a 10, ficando na 107ª posição, que confirma o que o estudo realizado apresenta: que a Lei de Acesso à Informação não está sendo cumprida totalmente pela Prefeitura Municipal de Travesseiro.

A partir deste ponto, onde as ameaças são conhecidas, sugere-se que seja feita uma análise de riscos especifica, assim como uma análise de vulnerabilidade dos mesmos com o objetivo de apontar as falhas bem como sugerir soluções.

Em função da relevância do tema em questão e objetivando aproximar as organizações que fazem uso das Tecnologias da Informação do ideal: estar de acordo com a Lei de Acesso à Informação e com a norma NBR ISO/IEC 17799, esta pesquisa poderá servir de base para trabalhos futuros desenvolvidos nesse sentido.

REFERÊNCIAS

ALBUQUERQUE, Ricardo; RIBEIRO, Bruno. **Segurança no desenvolvimento de software**: como desenvolver sistemas seguros e avaliar a segurança de aplicações desenvolvidas com base na ISO 15.408. Rio de Janeiro: Campus, 2002.

BEAL, Adriana. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2008.

BEAL, Adriana. **Gestão estratégica da informação**: como transformar a informação e a tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações. São Paulo: Atlas, 2012.

CRESWELL, John W.; ROCHA, Luciana de Oliveira. **Projeto de pesquisa**: métodos qualitativo, quantitativo e misto. 2. ed. Porto Alegre: Artmed, 2007.

DE SORDI, José Osvaldo; MEIRELES, Manuel. **Administração de sistemas de informação**: uma abordagem interativa. São Paulo: Saraiva, 2010.

Escala Brasil Transparente, Disponível em: <http://www.cgu.gov.br/assuntos/transparencia-publica/escala-brasil-transparente > Acesso em: 19 de maio de 2015.

DIAS, Claudia. **Segurança e auditoria da tecnologia da informação**. Rio de Janeiro: Axcel Books do Brasil, 2000.

Fontes, Edison, **Segurança da Informação: o usuário faz a diferença**, São Paulo, Saraiva, 2006.

GIBBS, Graham; COSTA, Roberto Cataldo. **Análise de dados qualitativos**. Porto Alegre: Artmed, 2009.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2012.

GONÇALVES, Carlos Alberto; MEIRELLES, Anthero de Moraes. **Projetos e relatórios de pesquisa em administração**. São Paulo: Atlas, 2004.

IMONIANA, Joshua Onome. **Auditoria de sistemas de informação**. 2. ed. São Paulo: Atlas, 2010.

KANAANE, Roberto; FIEL FILHO, Alécio; FERREIRA, Maria das Graças (Orgs). **Gestão pública**: planejamento, processos, sistemas de informação e pessoas. São Paulo: Atlas, 2010.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. 7. ed. São Paulo: Atlas, 2010.

Lei 12.527 de 18 de Novembro de 2011 - Lei de Acesso a Informação, Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm> Acesso em: 09 de março de 2015.

Manual da Lei de Acesso a Informação para Estados e Municípios, Disponível em: <http://www.cgu.gov.br/Publicacoes/transparencia-publica/brasil-transparente/arquivos/manual_lai_estadosmunicipios.pdf >, Acesso em 05 de maio de 2015.

NBR ISO/IEC 17799 - **Tecnologia da informação - técnicas de segurança**. 2. ed. Rio de Janeiro: ABNT, 2005.

REZENDE, Denis Alcides. **Planejamento de sistemas de informação e informática: guia prático para planejar a tecnologia da informação integrada ao planejamento estratégico das organizações**. São Paulo: Atlas, 2003.

YIN, Robert K. **Estudo de caso**: planejamento e métodos. 4. ed. Porto Alegre: Bookman, 2010.

ROSINI, Alessandro Marco; PALMISANO, Angelo. **Administração de sistemas de informação e a gestão do conhecimento**. 2. ed. rev. ampl. São Paulo: Cengage Learning, 2012.

ROESCH, Sylvia Maria Azevedo. **Projetos de estágio e de pesquisa em administração**: guia para estágios, trabalhos de conclusão, dissertações e estudos de caso. 3. ed. São Paulo: Atlas, 2005.

ROESCH, Sylvia Maria Azevedo. **Projetos de estágio do curso de administração**: guia para pesquisas, projetos, estágios e trabalho de conclusão de curso. São Paulo: Atlas, 1996.

SAMPIERI, Roberto Hernández; COLLADO, Carlos Fernández; LUCIO, Pilar Baptista. **Metodologia de pesquisa**. 3. ed. São Paulo: McGraw-Hill, 2006.

SÊMOLA, Marcos. **Gestão da segurança da informação**: visão executiva da segurança da informação: aplicada ao Security Officer. Rio de Janeiro: Elsevier, 2003.

TURBAN, Efraim; RAINER, R. Kelly; POTTER, Richard E. Administração de tecnologia da informação: teoria e pratica. Rio de Janeiro: Campus, 2003.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração**. 9. ed. São Paulo: Atlas, 2007.

APÊNDICE

Apêndice A – Grau de aderência à norma NBR ISO/IEC 17799

Este questionário servirá de auxílio para identificar o Grau de aderência à norma NBR ISO/IEC 17799.

Marque com “X” a resposta escolhida.

Grau de aderência à política de segurança da informação

Prática	Aderência		
	Sim	Sim, porém desatualizada	Não
Política de segurança?			
Algum responsável pela gestão da política de segurança?			

Grau de aderência à segurança organizacional

Prática	Aderência		
	Sim	Sim, porém desatualizada.	Não
Infraestrutura de segurança da informação para gerenciar as ações coorporativas?			
Fórum de segurança formado pelo corpo diretor, a fim de gerir mudanças estratégicas?			
Definição clara das atribuições de responsabilidade associadas à segurança da informação?			
Identificação dos riscos no acesso de prestadores de serviço?			
Controle de acesso específico para os prestadores de serviço?			
Requisitos de segurança dos contratos de terceirização?			

Grau de aderência à classificação e controle dos ativos

Prática	Aderência		
	Sim	Sim, porém desatualizada	Não
Inventário dos ativos físicos, lógicos e humanos?			
Critérios de classificação da informação?			

Grau de aderência à segurança em pessoas

Prática	Aderência		
	Sim	Sim, porém desatualizada	Não
Critérios de seleção e política de pessoal?			
Acordo de confidencialidade, termos e condições de trabalho?			
Processos para capacitação e treinamento de usuários?			
Estrutura para notificar e responder aos incidentes e falhas de segurança?			

Grau de aderência à segurança física e de ambiente

Prática	Aderência		
	Sim	Sim, porém desatualizada	Não
Definição de perímetros e controles de acesso físico aos ambientes?			
Recursos para segurança e manutenção dos equipamentos?			
Estrutura para fornecimento adequado de energia?			
Segurança do cabeamento?			

Grau de aderência ao gerenciamento das operações e comunicações

Prática	Aderência		
	Sim	Sim, porém desatualizada	Não
Procedimentos e responsabilidades operacionais?			
Controle de mudanças operacionais?			
Segregação de funções e ambientes?			
Planejamento e aceitação de sistemas?			
Procedimentos para cópias de segurança?			
Controles e gerenciamento de rede?			
Mecanismos de segurança e tratamento de mídias?			
Procedimentos para documentação de sistemas?			
Mecanismos de segurança do correio eletrônico?			

Grau de aderência ao controle de acesso

Prática	Aderência		
	Sim	Sim, porém desatualizada	Não
Requisitos do negócio para controle de acesso?			
Gerenciamento de acesso do usuário?			
Controle de acesso à rede?			
Controle de acesso ao sistema operacional?			
Controle de acesso às aplicações?			
Monitoração de uso e acesso ao sistema?			
Critérios para computação móvel e trabalho remoto?			

Grau de aderência ao desenvolvimento e manutenção de sistemas

Prática	Aderência		
	Sim	Sim, porém desatualizada	Não
Requisitos de segurança de sistemas?			
Controle de criptografia?			
Mecanismos de segurança nos processos de desenvolvimento e suporte?			

Grau de aderência á gestão de incidentes da segurança da informação.

Prática	Aderência		
	Sim	Sim, porém desatualizada	Não
Existe um processo formalizado e implantado para o tratamento dos incidentes?			
Existe uma estrutura responsável pelo tratamento dos incidentes?			

Grau de aderência à conformidade

Prática	Aderência		
	Sim	Sim, porém desatualizada	Não
Gestão de conformidade técnicas e legais?			
Recursos e critérios para auditoria de sistemas?			

Apêndice B – Aderência a Lei de Acesso a Informação.

Questionário sobre a Lei 12.527/2011, Lei de Acesso a Informação.

Escolha uma resposta para cada pergunta.

Em 18 de Novembro de 2011, foi decretada e sancionada pelo Congresso Nacional a Lei de Acesso a Informação. Conforme o Art. 1º, esta lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.

1. Você tem conhecimento da Lei 12.527/2011 que garante o Acesso a Informação para a população?

( ) Sim ( ) Sim, em parte ( ) Não

Conforme o Inciso I, do art. 1º da Lei 12.527/2011, os órgãos púbicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo Cortes de Contas, e Judiciário e do Ministério Publico, subordinam-se ao regime desta lei.

2. A Lei de Acesso a Informação é aplicada no setor em que você trabalha?

( ) Sim ( ) Sim, em parte ( ) Não

No art. 4º, inciso III da Lei temos:

III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

3. As informações geradas no setor requer Sigilo?

( ) Sim ( ) Sim, em parte ( ) Não

No art. 31 da Lei consta que:

I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e

II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

§ 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.

4. As informações de cunho pessoal são tratadas de acordo com a Lei?

( ) Sim ( ) Sim, em parte ( ) Não

Os prazos estão relacionados ao paragrafo primeiro e seus incisos do art. 24, que diz:

§ 1º Os prazos máximos de restrição de acesso à informação, conforme a classificação prevista no **caput**, vigoram a partir da data de sua produção e são os seguintes:

I - ultrassecreta: 25 (vinte e cinco) anos;

II - secreta: 15 (quinze) anos; e

III - reservada: 5 (cinco) anos.

5. São conhecidos os prazos de cada classificação?

( ) Sim ( ) Sim, em parte ( ) Não

Conforme o art. 25 da Lei, § 2º O acesso à informação classificada como sigilosa cria a obrigação para aquele que a obteve de resguardar o sigilo.

6. Você sabe das obrigações sobre a guarda de sigilo?

( ) Sim ( ) Sim, em parte ( ) Não

No art. 4º da Lei, são definidos importantes conceitos, que são considerados para efeitos desta Lei, conforme segue os incisos VI, VII, VIII e IX:

VI - **disponibilidade**: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

VII - **autenticidade**: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

VIII - **integridade**: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;
IX - **primariedade**: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

7. As informações geradas no seu setor obedecem aos princípios da disponibilidade?
( ) Sim ( ) Sim, em parte ( ) Não
8. As informações geradas no seu setor obedecem aos princípios da autenticidade?
( ) Sim ( ) Sim, em parte ( ) Não
9. As informações geradas no seu setor obedecem aos princípios da integridade?
( ) Sim ( ) Sim, em parte ( ) Não
10. As informações geradas no seu setor obedecem aos princípios da primariedade?
( ) Sim ( ) Sim, em parte ( ) Não

No art. 32, Inciso II e § 2º a lei fala das responsabilidades dos agentes públicos perante as condutas ilícitas.
II - para fins do disposto na Lei nº 8.112, de 11 de dezembro de 1990, e suas alterações, infrações administrativas, que deverão ser apenadas, no mínimo, com suspensão, segundo os critérios nela estabelecidos.
§ 2º (...) poderá o agente público responder, também, por improbidade administrativa, conforme o disposto nas Leis nº 1.079, de 10 de abril de 1950, e n° 8.429, de 2 de junho de 1992.

11. Você sabe das responsabilidades sofridas pelo agente público, por conduta ilícita com as informações?
( ) Sim ( ) Sim, em parte ( ) Não

No atr. 8º a lei prevê que:

§ 2º (...) os órgãos e entidades públicas deverão utilizar todos os meios e instrumentos legítimos de que dispuserem, sendo obrigatória a divulgação em sítios oficiais da rede mundial de computadores (internet).

§ 3º Os sítios de que trata o § 2º deverão, na forma de regulamento, atender, entre outros, aos seguintes requisitos:

II - possibilitar a gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações;

III - possibilitar o acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina;

IV - divulgar em detalhes os formatos utilizados para estruturação da informação;

V - garantir a autenticidade e a integridade das informações disponíveis para acesso;

VI - manter atualizadas as informações disponíveis para acesso;

12. As informações são disponibilizadas em sítios oficiais?

( ) Sim ( ) Sim, em parte ( ) Não

13. As informações disponibilizadas nos sítios oficiais são de formato padronizado?

( ) Sim ( ) Sim, em parte ( ) Não

14. As informações disponibilizadas nos sítios oficiais são seguras?

( ) Sim ( ) Sim, em parte ( ) Não

15. As atualizações das informações nos sítios oficiais são constantes?

( ) Sim ( ) Sim, em parte ( ) Não

Conforme o art. 45 da Lei cabe aos Estados, ao Distrito Federal e aos Municípios, em legislação própria, obedecidas as normas gerais estabelecidas nesta Lei, definir regras específicas, especialmente quanto ao disposto no art. 9º e na Seção II do Capítulo III.

16. Existe regulamentação própria definindo regras especificas visando a segurança da informação?

( ) Sim ( ) Sim, em parte ( ) Não

Conforme o art. 6º da Lei cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a:

I - gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação;

II - proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e

III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

17. Foi realizado treinamento sobre o acesso a informação?

( ) Sim ( ) Sim, em parte ( ) Não

18. As informações geradas no setor são auditadas?

( ) Sim ( ) Sim, em parte ( ) Não

Apêndice C – Percepção dos funcionários

Na sua percepção, responda o questionário abaixo, marcando uma das alternativas.

1. O acesso à informação da Prefeitura Municipal de Travesseiro está de acordo com a Lei e com as boas práticas de Tecnologia da Informação?
   ( ) Sim ( ) Sim, em parte ( ) Não

2. A disponibilização das informações está obedecendo ao formato padronizado?
   ( ) Sim ( ) Sim, em parte ( ) Não

3. A guarda das informações é segura?
   ( ) Sim ( ) Sim, em parte ( ) Não

4. O site no qual as informações são disponibilizadas é seguro?
   ( ) Sim ( ) Sim, em parte ( ) Não

5. A Prefeitura Municipal de Travesseiro está de acordo com as boas praticas de segurança da informação?
   ( ) Sim ( ) Sim, em parte ( ) Não