UNIVERSIDADE DE CAXIAS DO SUL

ÁREA DO CONHECIMENTO DE CIÊNCIAS EXATAS E ENGENHARIAS

RAFAEL MOLIN

LEI 13.709: UMA ANÁLISE DOS ASPECTOS TÉCNICOS INFORMÁTICOS

CAXIAS DO SUL

2019

RAFAEL MOLIN

LEI 13.709: UMA ANÁLISE DOS ASPECTOS TÉCNICOS INFORMÁTICOS

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título de Bacharel em Sistemas de Informação na Área do Conhecimento de Ciências Exatas e Engenharias da Universidade de Caxias do Sul.

Orientador: Prof. Dra. Maria de Fátima Webber do Prado Lima
Coorientador: Prof. Ma. Patrícia Montemezzo

CAXIAS DO SUL

2019

RAFAEL MOLIN

LEI 13.709: UMA ANÁLISE DOS ASPECTOS TÉCNICOS INFORMÁTICOS

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título de Bacharel em Sistemas de Informação na Área do Conhecimento de Ciências Exatas e Engenharias da Universidade de Caxias do Sul.

Aprovado em 24/06/2019

Banca Examinadora

_____

Prof. Dra. Maria de Fátima Webber do Prado Lima
Universidade de Caxias do Sul

_____

Prof. Me. Giovanni Ely Rocco
Universidade de Caxias do Sul

_____

Prof. Ma. Iraci Cristina da Silveira de Carli
Universidade de Caxias do Sul

RESUMO

A evolução das tecnologias de informação e da comunicação trouxe diversas facilidades para as pessoas. Hoje, muitos serviços são prestados, tanto por entidades públicas como privadas, de forma prática e rápida, utilizando meios digitais, como compras, inscrições em diversos tipos de eventos e transações bancárias. Muitos destes serviços solicitam dados pessoais, os quais são fornecidos e, nem sempre, é sabido como estes são mantidos em segurança posteriormente. Com o objetivo de regulamentar a maneira como os dados pessoais são tratados pelas empresas, foi aprovada a Lei 13.709/18, apresentando seus deveres e responsabilidades. Desta forma, foi desenvolvido este trabalho, através de uma análise técnica na Lei 13.709/18, buscando identificar os requisitos técnicos de segurança da informação da mesma. A análise de três estudos de caso foi utilizada para validar os requisitos identificados, o que proporcionou a percepção de que as empresas precisam melhorar seus processos de gerenciamento da segurança da informação, não somente por requisito da Lei 13.709, mas por manter práticas e procedimentos que sejam eficazes para eliminar ou diminuir prejuízos por incidentes de quebra de segurança.

Palavras-chave: Legislação; Dados Pessoais; Segurança da Informação; Privacidade.

ABSTRACT

The evolution of information and communication technologies has been making everyday's activities easier. Nowadays, many services are provided by both public and private entities using digital means, such as shopping, enrollment in various types of events and banking transactions. Most of these services request personal data, what rises questions on how safe is this information storage. Brazil has approved Law 13.709/2018 with the purpose of regulating how companies should manage personal data, in addition to clarifying their duties and responsibilities. Thus, this work was developed with the technical analysis of Law 13.709/18, to identify the technical requirements of information security. The analysis of three case studies was used to validate the identified requirements, providing the perception that companies need to improve their processes of information security management. This process doesn't only refer to Law 13.709/18, but also to maintain practices that are effective in eliminating or reducing damages from information security breachs.

Keyword: Legislation; Personal Data; Information Security; Privacy.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

CEO	*Chief Executive Officer* (Diretor Executivo)
DoS	*Denial of Service*
ESP	*Encrypted Security Payload*
IDS	*Intrusion detection system*
IPv6	*Internet Protocol version 6*
ISO	*International Organization of Standardization*
PIN	*Personal Identification Number*
PGP	*Pretty Good Privacy*
PSI	Política de Segurança da Informação
RGPD	Regulamento Geral de Proteção de Dados da União Europeia
SGSI	Sistema de Gestão de Sistemas de Informação
SSL	*Security Socket Layer*
TI	Tecnologia da informação
VPN	*Virtual Private Network*

SUMÁRIO

1 INTRODUÇÃO

A interação entre pessoas e tecnologias tem aumentado de forma rápida e generalizada nos últimos anos. Paralelamente, a quantidade de dados pessoais em poder de organizações é muito grande. A facilidade com que se fornece tais informações às organizações gera um problema cada vez mais preocupante: o acesso indevido e o vazamento de informações.

Como todo ativo, a informação deve ser considerada segura, e, para isso, deve ser confidencial, íntegra e disponível (FOROUZAN, MOSHARRAF, 2013). A confidencialidade determina que a informação deve ser protegida de acessos não autorizados e ataques. A integridade significa que os dados devem manter seu estado original, sem alterações indevidas. A disponibilidade, por sua vez, permite que a informação deve estar disponível para acesso autorizado sempre que necessário. Com o crescente advento da comunicação entre diversos dispositivos, esses requisitos – confidencialidade, integridade e disponibilidade – ganham uma nova dimensão, observando que não se tratam apenas de informações de organizações, mas também, de indivíduos que podem ter seus direitos de privacidade corrompidos se não forem tomadas as devidas medidas de segurança em armazenamento e tratamento de dados.

Episódios envolvendo vazamento de dados são cada vez mais comuns e a forma de tratá-los torna-se um desafio. O Brasil é um dos países com maior incidência em vazamento de dados pessoais na *deepweb*. Pesquisa da Psafe (COMPUTERWORLD, 2016), empresa de segurança e desempenho de dispositivos móveis, aponta que cerca de 50 milhões de usuários no mundo tiveram dados vazados ou roubados por *hackers*, entre eles, 20 mil autoridades governamentais. Segundo essa mesma pesquisa, o Brasil está em segundo lugar no *ranking* de países mais afetados, perdendo apenas para os Estados Unidos, com 1,2 milhões de usuários expostos.

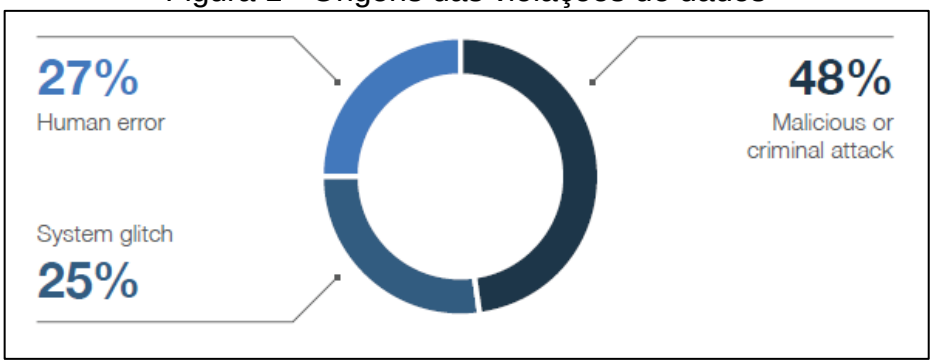
Recentemente, a empresa SonicWall emitiu relatório que alerta sobre ameaças de sequestro de dados (*ransomwares*). Segundo a empresa, os ataques desse tipo tiveram uma queda significativa entre 2016 e 2017, mas cresceram cerca de 229% no

primeiro semestre de 2018, comparado ao mesmo período de 2017 (COMPUTERWORLD, 2018).

Um caso que obteve repercussão negativa foi o vazamento de dados de usuários do Facebook, por meio de um teste de personalidade, que afetou cerca de 87 milhões de usuários da rede social. Esse episódio causou uma queda de 6,8% nas ações da empresa, ocasionando uma perda de aproximadamente US$ 95 bilhões em valor de mercado (COMPUTERWORLD, 2018). Além disso, o CEO do Facebook, Mark Zuckerberg, foi convocado a esclarecer o fato diante do Comitê Judiciário e de Comércio do Senado dos Estados Unidos, respondendo questões sobre regulação, uso de dados de usuários e como a empresa reagiu após o incidente (EXAME, 2018).

Na tentativa de demonstrar o valor financeiro de problemas de segurança, a empresa Ponemon Institute realiza um levantamento anual dos custos de vazamentos de dados em empresas do mundo inteiro (IBM NEWS ROOM, 2018). No relatório emitido em 2018, o estudo demonstrou que o custo médio global de uma violação de dados é de US$ 3,86 milhões. Este mesmo estudo também mostra que a maioria das violações acontece por meio de ataques maliciosos ou criminosos, conforme demonstrado na Figura 1. Os eventos de vazamentos de dados e quebra de segurança trazem um novo desafio para as organizações, no que diz respeito a manter a informação gerada, recebida e tratada de maneira segura.

Figura 1 - Origens das violações de dados



Fonte: Ponemom Institute (2018)

Além de perdas financeiras, os dados e informações que as empresas possuem em seu poder podem oferecer riscos à individualidade e privacidade das pessoas que, de alguma forma, consentem em oferecer tais informações. Os casos de falhas em Segurança da Informação que permitem a exposição indevida de dados pessoais

levaram a União Europeia a reforçar a proteção de dados dos cidadãos da Europa criando a RGPD (Regulamento Geral de Proteção de Dados da União Europeia), projeto de lei que entrou em vigor no dia 25 de maio de 2018. Essa norma prevê diretrizes de como as empresas devem tratar os dados privados de seus clientes, envolvendo três pilares: transparência, gestão e governança (TECMUNDO, 2018). Apesar de vários países europeus já possuírem legislações sobre segurança de dados, não correspondiam ao cenário tecnológico atual. Com a criação de regras rígidas para coleta, processamento, compartilhamento e resguardo de dados pessoais, a União Europeia procura fazer com que as empresas sejam mais transparentes no que diz respeito à utilização de dados pessoais, além de cobrar maior responsabilidade em casos de vazamento ou violação dos mesmos.

Seguindo essa tendência, um projeto de lei similar foi sancionado no Brasil pelo Presidente da República. A Lei 13.709 de 14 de agosto de 2018 dispõe sobre a proteção de dados pessoais, alterando a Lei 12.965 de 23 de abril de 2014 (Marco Civil da Internet) (BRASIL, 2018). A preocupação com a segurança dos dados fornecidos pelas pessoas para organizações atinge outro patamar, pois, até o momento, não existia nenhuma legislação que tratasse desse assunto a nível nacional.

1.1 PROBLEMA DE PESQUISA

A segurança de dados em poder de organizações, a nível mundial, é um assunto muito abordado atualmente. Notícias sobre vazamento ou quebra de segurança de dados pessoais circulam com grande frequência, como dados de redes sociais e instituições financeiras, inclusive no Brasil.

A Lei 13.709 visa a regulamentação das informações pessoais no âmbito organizacional, seja no poder público ou privado. Além de questões puramente jurídicas, como regras sobre como as empresas devem solicitar o consentimento ao titular sobre a manutenção de seus dados, existem requisitos técnicos de segurança da informação, os quais as organizações devem ter implantados, minimamente, em sua estrutura de TI.

Diante do exposto, é necessário que as organizações se adéquem às regras impostas na nova legislação.

Questão de pesquisa: Quais são as mudanças necessárias, na área de Tecnologia da Informação, que devem ser efetuadas nas organizações para que elas cumpram a Lei nº 13.709?

1.2 OBJETIVO

O objetivo deste trabalho é realizar uma análise técnica da Lei 13.709, verificando quais ferramentas e medidas de segurança da informação devem ser adotadas pelas organizações para atender os requisitos legais dispostos na Lei.

Os objetivos específicos desse trabalho são:

a) Compreender os aspectos jurídicos da Lei nº 13.709 de 14/08/18;

b) Compreender quais os requisitos de segurança de informação que as diversas empresas terão que implantar para atender à nova lei;

c) Analisar tecnicamente quais são os mecanismos de segurança que as empresas precisarão implantar;

d) Realizar um estudo de caso em organizações para validar a análise técnica da nova Lei e obter um panorama de como as empresas estão se adequando a mesma.

1.3 METODOLOGIA

Para a realização deste trabalho, foi necessário compreender os aspectos jurídicos da Lei 13.709 de 14/08/2018, paralelamente com uma pesquisa bibliográfica, constituída principalmente de livros, artigos de periódicos e normas de segurança da informação, além de materiais disponibilizados na internet.

Em um segundo momento, foi realizado um estudo para compreender quais os requisitos de segurança de informação que as diversas empresas deverão considerar para atender aos pontos dispostos na nova lei.

Após, na terceira etapa, um novo estudo foi realizado, visando analisar tecnicamente quais os mecanismos de segurança que as empresas precisariam implantar minimamente para o atendimento à nova lei.

Como resultado desse estudo, foram avaliadas quais técnicas e práticas de Segurança da Informação, Segurança de Redes de Computadores e de Gestão de Sistemas de Informação poderiam ser adotadas para o atendimento efetivo dos requisitos da nova lei.

Na quarta etapa, foram selecionadas organizações, a fim de realizar um estudo de caso para validar a análise técnica da lei, verificando se a empresa realizava proteção de dados e como realizava. A coleta de dados ocorreu através de questionários estruturados, abordando como estavam implantadas as soluções necessárias para o atendimento à Lei. Questionários são utilizados para coleta de dados de informantes pré-selecionados. São respondidos, geralmente, sem a presença do pesquisador, visando levantamento de dados diretos, com questões e respostas estruturadas previamente, buscando formar escalas para posterior avaliação (MARTINS, 2008). Após a coleta de dados, foi desenvolvido um panorama de como as empresas possuíam conhecimento e estavam preparadas para atender aos requisitos da Lei, comparando os resultados das pesquisas desenvolvidas com as necessidades levantadas em pesquisa bibliográfica. A partir desta comparação, foram apresentadas propostas cabíveis a cada organização estudada, com o objetivo do atendimento dos requisitos de segurança da informação abordados na Lei 13.709.

Após a apreciação das propostas pelas organizações, foi aplicada nova pesquisa, em formato de entrevistas. Entrevistas são importantes para evidenciar ações comportamentais e assuntos humanos (YIN, 2015), apresentando abordagens relevantes que os questionários podem não evidenciar. Além disso, podem ajudar a identificar outras fontes de informação com relevância, as quais não estavam definidas no roteiro da entrevista.

A escolha dos métodos se baseou em pesquisa de outros trabalhos acadêmicos que propõem um estudo de caso em organizações para validação de hipóteses propostas (ZANELLA, 2017; BASTOS, 2006; MEDEIROS, 2016; SCHIER, 2009). Ambos os trabalhos utilizaram o método de estudos de caso com caráter exploratório, buscando evidenciar e aprofundar o conhecimento sobre fenômenos específicos dentro das organizações para, posteriormente, gerar um diagnóstico mais apurado de cada uma das organizações que, aliado a estudos bibliográficos, auxiliaram na proposição de soluções específicas para questões previamente definidas.

No caso deste trabalho, esperava-se que, com as pesquisas iniciais, se obtivesse um panorama da situação atual, com possíveis faltas de ferramentas ou medidas de segurança que fossem necessárias para atender aos requisitos da Lei 13.709. Esse primeiro levantamento de dados também foi útil para evidenciar a preparação de forma geral que as empresas possuem para atender tais requisitos. Após a análise destes dados, uma proposta foi apresentada a cada uma das organizações pesquisadas, a fim de indicar quais as alterações seriam necessárias em seus sistemas de informação, no que diz respeito a segurança da informação, para atendimento dos requisitos da Lei. Após, com a realização da pesquisa final (entrevistas em cada uma das organizações), esperava-se identificar a aceitação que cada uma das organizações teria em relação às alterações propostas em suas medidas de segurança, e as adaptações necessárias para atender as normas estabelecidas na Lei 13.709.

1.4 ESTRUTURA DO TRABALHO

O Capítulo 2 deste trabalho apresenta um resumo da Lei 13.709, abordando os requisitos impostos pela mesma, como também as responsabilidades e deveres dos envolvidos.

O Capítulo 3, denominado Mecanismos, sistemas e ferramentas de segurança da informação, descreve as principais ameaças que abordam a Lei 13.709, conforme literatura. Apresenta medidas e ferramentas de segurança da informação que podem ser aplicadas em organizações, relacionadas aos requisitos impostos pela Lei.

O Capítulo 4 aborda a elucidação da proposta de solução para o problema pesquisa apresentado no Capítulo 1 deste trabalho, com a metodologia utilizada para realizar os estudos de caso e a coleta de dados para realizar as etapas posteriores deste trabalho.

O Capítulo 5, por fim, apresenta os resultados obtidos na realização do trabalho, contendo as análises dos estudos de caso e a percepção de cada empresa quanto as sugestões de melhoria apresentadas.

Por último, o Capítulo 6 apresenta a conclusão final deste trabalho.

2 LEI N° 13.709

A Lei n° 13.709 refere-se ao marco legal de proteção, tratamento e uso de dados pessoais no Brasil, visando um controle maior dos indivíduos sobre suas informações pessoais em poder de organizações.

Esse capítulo apresenta um resumo da Lei 13.709. A Seção 2.1 resume as disposições preliminares sobre a nova Lei. A Seção 2.2 apresenta as regras para realização do tratamento de dados. A Seção 2.3 mostra os direitos assegurados ao titular dos dados. A Seção 2.4 refere-se ao tratamento de dados pelo Poder Público. A Seção 2.5 define as regras para a transferência internacional de dados pessoais. A Seção 2.6 explica as responsabilidades dos agentes responsáveis pelo tratamento dos dados. A Seção 2.7 indica os requisitos de segurança e boas práticas para armazenamento e tratamento de dados. Por fim, a Seção 2.8 apresenta as considerações parciais referentes aos requisitos impostos pela nova Lei.

Para entendimento das responsabilidades e deveres, considera-se, no decorrer desse capítulo, as seguintes definições:

a) titular: pessoa natural a quem se refere os dados pessoais;

b) controlador: pessoa natural ou jurídica, a quem compete as decisões sobre o tratamento dos dados;

c) operador: pessoa natural ou jurídica que realiza o tratamento dos dados em nome do controlador;

d) encarregado: pessoa natural, indicada pelo controlador, que atua como canal de comunicação entre controlador e titulares, ou entre controlador e a autoridade nacional.

2.1 DISPOSIÇÕES PRELIMINARES

A Lei 13.709 dispõe sobre o tratamento de dados pessoais, realizado por empresas privadas ou públicas, bem como por pessoa física, a fim de proteger os direitos legítimos de privacidade e liberdade das pessoas.

Na presente seção ficam claros os pontos em que a lei se fundamenta, no que diz respeito aos direitos fundamentais do cidadão, como privacidade, liberdade de

expressão, informação, inviolabilidade da intimidade, honra e da imagem. Também trata dos fundamentos coletivos, como o desenvolvimento econômico e tecnológico, a livre iniciativa e a livre concorrência, defesa do consumidor e os direitos humanos.

Alguns princípios devem ser observados para o cumprimento da Lei. A finalidade da realização do tratamento de dados deve ter propósitos legítimos. O titular deve ser informado sobre tais finalidades, de forma explícita, não podendo ocorrer tratamento além disso. Os meios de tratamento devem ser adequados a finalidade definida e informada ao titular, sendo o tratamento limitado ao mínimo necessário para tal finalidade. O titular deve ter acesso garantido e facilitado sobre a forma e a duração do tratamento, e a qualidade dos dados deve ser garantida quanto a exatidão, clareza, relevância e atualização, conforme a finalidade proposta. A segurança dos dados deve ser garantida, com observância às medidas técnicas e administrativas para tal, protegendo-os de ataques e vazamentos não autorizados. As medidas de segurança adotadas devem ser, sempre que solicitado, disponibilizadas pelos agentes de tratamento, demonstrando que existe o cumprimento dos requisitos da Lei.

2.2 REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS

As regras e condições para aplicação da Lei são válidas para qualquer tipo de tratamento de dados, por empresa nacional ou não, de direito público ou privado, ou também, por pessoa física, desde que o tratamento seja realizado em território nacional, voltado para o fornecimento de produto ou serviço ou os dados haverem sido coletados, ambos, em território nacional. Entende-se por tratamento de dados pessoais um conjunto de operações efetuadas sobre os mesmos, de forma manual ou automatizada, que inclui coleta, registro, organização, estruturação, conservação, alteração, recuperação, consulta, utilização, divulgação, difusão, comparação, eliminação ou destruição.

Existem exceções para a aplicação da Lei, como nos casos em que o tratamento for realizado por pessoa natural para fins particulares e não econômicos, ou em fins exclusivamente jornalísticos, artísticos ou acadêmicos (desde que exista o consentimento do titular). Também estão excluídas as regras da Lei nos casos em que a finalidade do tratamento for para segurança pública, defesa nacional, segurança do Estado ou atividade de investigação.

Dentre as hipóteses aceitas para o tratamento dos dados, a primeira e principal diz respeito ao consentimento explícito do titular para tal. Tal consentimento deve ser fornecido de forma escrita, ou por outro meio, demonstrando explicitamente a vontade do mesmo. O consentimento deve prever a finalidade do tratamento, e pode ser revogado a qualquer momento mediante manifestação do titular. Porém, também pode haver o tratamento para cumprimento de obrigações legais, ou pela administração pública, na execução de políticas públicas previstas em leis e regulamentos, desde que o titular seja informado previamente sobre o tratamento. Cabe ressaltar que, mesmo após o consentimento do titular, se houver necessidade de compartilhamento de dados com outros controladores ou agentes, é necessário solicitar novo consentimento, explicitando as finalidades para tal.

Para fins de pesquisa, os órgãos responsáveis podem efetuar o tratamento, desde que, sempre que possível, seja garantida a anonimização[1] dos dados pessoais.

O tratamento dos dados pode ocorrer com a finalidade de garantir a segurança, proteção da vida e a tutela da saúde em procedimentos realizados por profissionais pertinentes, bem como em casos onde caiba a proteção do crédito, sempre respeitando os direitos de privacidade do titular.

O titular deve ter acesso facilitado as informações que dizem respeito ao tratamento dos dados pessoais disponibilizados. Devem estar disponíveis as seguintes informações: finalidade do tratamento, duração e forma do tratamento, identificação do controlador, informações sobre compartilhamento de dados (quando existir), responsabilidades dos agentes de tratamento e direitos do titular dos dados.

Quando o tratamento de dados for para interesse legítimo do controlador, o mesmo deve manter somente os dados estritamente necessários para tal. Também devem ser adotadas medidas para garantir a transparência das informações de tratamento.

O tratamento de dados de crianças e adolescentes deverá ser realizado somente para exercer interesses restritamente necessários, em sua melhor hipótese

[1] Anonimização é o processo de alteração da informação armazenada em um banco de dados, com a finalidade de dificultar ou impedir a identificação do indivíduo titular desta. Esse processo pode acontecer por meio de técnicas que eliminam a identificação, não permitindo sua reversão, ou por meios que apenas ofuscam a identificação, permitindo uma posterior reversão.

e obedecendo legislação pertinente. Deve existir consentimento específico e em destaque dado por, pelo menos, um dos pais ou responsável legal.

A coleta de dados sem o consentimento é permitida em casos específicos, como quando feita para contatar os pais ou responsável legal, sem que haja o armazenamento desses dados.

Em resumo, o capítulo II apresenta regras para a realização do tratamento de dados, as quais dizem respeito a adoção de medidas administrativas para explicitar o consentimento do titular sobre a utilização dos dados pessoais ou, se não por esse meio, quais devem ser adotados de forma legal para a realização do tratamento.

2.2.1 Tratamento de dados pessoais sensíveis

Dados sensíveis são aqueles que trazem informações adicionais sobre opinião ou caráter do titular (raça, etnia, religião, opinião política, dados referentes à saúde ou vida sexual, dados genéticos ou biométricos). Os requisitos para tratamento destes dados são similares às regras para dados pessoais, com ressalvas nos casos de dados coletados para pesquisa, onde é solicitada a anonimização dos mesmos.

Quando existir o processo de anonimização, os dados deixam de ser considerados pessoais perante a Lei 13.709. Porém, se estes dados forem submetidos a uma reversão, voltam a se enquadrar nos requisitos propostos na Lei.

Os dados utilizados para formação de perfil comportamental em uma seleção de emprego, por exemplo, são considerados dados sensíveis e devem seguir os requisitos da Lei. No momento da divulgação de resultado de pesquisa não devem ser expostos, em nenhuma hipótese, os dados pessoais extraídos para tal, seguindo a regra da anonimização.

2.2.2 Término do Tratamento

Conforme os requisitos da Lei, o tratamento dos dados pessoais deve possuir um ponto que se caracteriza por sua finalização. O término do tratamento pode ocorrer quando a finalidade desejada for alcançada, ou período para tratamento estipulado no ato do consentimento pelo titular se encerrar, ou quando houver comunicação por

parte do titular, expressando seu direito de revogar o consentimento, antes fornecido, para o tratamento.

Após o término do tratamento, os dados pessoais devem ser eliminados. Porém, podem ser conservados em casos de pesquisa, ou uso restrito do controlador, desde que sejam anonimizados.

2.3 DIREITOS DO TITULAR

Toda pessoa tem assegurada a titularidade de seus dados pessoais, como também seus direitos fundamentais previstos em lei.

O titular tem o direito de solicitar, a qualquer momento, as seguintes informações perante o controlador do tratamento de dados:

a) confirmação da existência do tratamento;

b) acesso aos dados armazenados;

c) correção ou atualização de dados armazenados;

d) anonimização, bloqueio ou eliminação de dados desnecessários;

e) portabilidade de dados, desde que exista requisição expressa para tal;

f) eliminação dos dados, respeitando os requisitos dispostos na Lei;

g) informação das entidades públicas e privadas com as quais existiu uso compartilhado de dados;

h) informação sobre a possibilidade de não consentimento para uso dos dados e as consequências caso isso ocorra;

i) revogação do consentimento, conforme regras dispostas na Lei.

O titular pode requerer seus direitos sem nenhum custo por parte do controlador. Quando houver uso compartilhado de dados, o responsável deve informar imediatamente aos agentes que usam deste compartilhamento sobre qualquer alteração ou atualização nos dados do titular.

O acesso a dados pessoais ou informações sobre o tratamento devem ser providenciados de forma simplificada (imediatamente), ou completa, incluindo a

origem dos dados, critérios de tratamento, no prazo de quinze dias a contar da data de solicitação.

O armazenamento de dados precisa ser feito de forma a facilitar o fornecimento de informações quando solicitado pelo titular. Essas informações podem ser fornecidas de forma impressa ou por meio eletrônico. No caso de utilização deste último, os dados devem ser transferidos de maneira idônea e segura. Nesse caso, o controlador deve observar quais as ferramentas necessárias para realizar o envio, uma vez que deve ser um processo prático para o titular e, ao mesmo tempo, eficaz no que diz respeito à segurança da informação. O titular pode, também, solicitar, de forma integral, cópia dos dados pessoais em poder do controlador. Essa cópia deve ser entregue em formato que favoreça utilização subsequente, inclusive, em outras operações de tratamento.

Nos casos de tratamento automatizado dos dados fornecidos, o titular tem direito a solicitar revisão dos critérios utilizados para tal, inclusive, quando se trata de definição de perfil pessoal e profissional, de consumo e de crédito. O controlador deve disponibilizar, quando solicitado, informações claras e adequadas a respeito dos critérios utilizados para realizar o tratamento automatizado dos dados.

Os dados pessoais fornecidos pelo titular não podem, em hipótese alguma, ser utilizados em seu prejuízo.

2.4 TRATAMENTO DE DADOS PELO PODER PÚBLICO

O tratamento de dados pessoais por pessoa jurídica de direito público deverá ser realizado somente com a finalidade de exercer atividades do interesse público, competências legais e atribuições voltadas ao serviço público.

É necessário informar claramente a finalidade, procedimentos adotados, previsão legal e práticas utilizadas para o tratamento dos dados. Essas informações devem ser de fácil acesso, preferencialmente, no site da instituição pertinente.

Serviços exercidos por empresas de caráter privado, como cartórios de serviço notariais e registro, por delegação do poder público, terão o mesmo tratamento de empresas de direito público. Estas instituições devem fornecer acesso aos seus dados, por meio eletrônico, para o poder público.

Empresas públicas e sociedades de economia mista, que atuam em regime de concorrência, serão tratadas como empresas de direito privado pelos termos da Lei. No caso de exercerem políticas públicas, serão, então, tratadas como empresas de direito público.

As entidades de direito público devem manter os dados de forma interoperável e estruturados de forma a facilitar seu uso compartilhado. O compartilhamento de dados deve respeitar as finalidades específicas para execução de políticas públicas. O poder público somente pode compartilhar dados pessoais com empresas de direito privado quando sua finalidade for, exclusivamente, a execução de políticas públicas, e nos casos em que os dados forem acessíveis publicamente. Quando houver compartilhamento de dados pessoais pelo poder público à pessoa de direito privado, é necessário informar a autoridade nacional, bem como dependerá do consentimento explícito do titular.

A autoridade nacional pode solicitar, a qualquer momento, informações pertinentes ao tratamento de dados pessoais às entidades do poder público. Sendo assim, é importante manter atualizados registros das atividades de tratamento, bem como, informações de registros, autorização, alteração ou eliminação de dados pessoais e a finalidade para o qual esses dados são utilizados.

2.5 TRANSFERÊNCIA INTERNACIONAL DE DADOS

A transferência internacional de dados pessoal somente poderá ocorrer quando forem garantidas as normas estipuladas na Lei. Para isso, a transferência somente é permitida nos seguintes casos:

a) para países que proporcionem grau de proteção de dados conforme previsto na Lei;

b) quando o controlador garantir e comprovar, através de contratos, normas corporativas ou selos, certificados e códigos de conduta, que cumpre os requisitos da Lei;

c) quando a finalidade do tratamento for a cooperação jurídica internacional ou a proteção da vida do titular ou terceiro;

d) sob autorização da autoridade nacional;

e) quando o resultado for compromisso assumido em acordo de cooperação internacional;

f) para cumprimento de políticas públicas ou atribuições legais;

g) sob o consentimento específico do titular, com informação explícita da finalidade do tratamento.

Cabe à autoridade nacional a avaliação do nível de proteção de dados do país estrangeiro ou organismo internacional alvo de transferência de dados, observando as normas da legislação em vigor no país de destino, a natureza dos dados, os princípios previstos na Lei e o amparo jurídico para o respeito dos direitos de proteção de dados pessoais.

A autoridade nacional deverá definir e avaliar conteúdo de cláusulas contratuais específicas para transferência de dados. A mesma também é responsável por verificar e avaliar normas e certificados que atendam aos requisitos da Lei. Pode existir a designação de órgãos certificadores para realizar a análise da transferência internacional de dados.

2.6 RESPONSABILIDADE DOS AGENTES DE TRATAMENTO

Os agentes de tratamento (controlador, operador e encarregado) possuem responsabilidades e atribuições específicas perante a Lei. Em comum, eles devem manter registro das operações de tratamento realizadas, principalmente quando baseadas no legítimo interesse. Entretanto, cada um tem funções individuais, conforme apresentado no decorrer desta seção.

O controlador, por manter informações pertinentes ao tratamento dos dados, pode ser solicitado, a qualquer momento, pela autoridade nacional, quanto à emissão de relatório de impacto à proteção de dados. O relatório deverá conter, no mínimo, descrição do tipo de dados coletados, metodologia utilizada na coleta e na segurança das informações, como, também, a análise do controlador quanto às medidas adotadas para mitigação de riscos.

O operador deve realizar o tratamento de dados somente segundo as instruções fornecidas pelo controlador, não podendo agir de maneira diferente, sob pena das sanções dispostas na Lei.

O encarregado, por sua vez, é responsável pela comunicação com os titulares, aceitando reclamações, inclusive, tomando as devidas providências. Também recebe comunicações da autoridade nacional, tomando as providências cabíveis. Deve orientar os funcionários e contratados da organização a respeito das práticas a ser adotadas quanto à proteção de dados pessoais. A identidade e informações de contato do encarregado devem estar disponíveis publicamente, de preferência, no site do controlador.

2.7 SEGURANÇA E BOAS PRÁTICAS

A Lei apresenta, em seu capítulo sobre Segurança e Boas Práticas, aspectos que devem ser respeitados no que diz respeito à garantia da inviolabilidade dos dados pessoais, a partir da adoção de medidas técnicas e administrativas, com a finalidade de proteger os dados de:

a) acessos não autorizados;

b) situações acidentais ou ilícitas de destruição de dados;

c) perda, alteração, vazamento ou qualquer forma de tratamento inadequado ou ilícito.

Devem ser observadas todas as medidas técnicas e administrativas cabíveis para manter a infraestrutura e os dados armazenados de maneira segura, mesmo após o término do tratamento dos dados.

O controlador deve informar à autoridade nacional sobre qualquer ocorrência de incidente de segurança. Deve ser informado, então:

a) qual a ocorrência;

b) informações sobre os titulares envolvidos no incidente;

c) as medidas de segurança utilizadas para proteção dos dados;

d) os riscos relacionados com o incidente;

e) motivos da demora para comunicação do incidente, se acaso ocorrer;

f) meios para mitigar ou reverter os efeitos do prejuízo.

A Lei também permite que os controladores e operadores, individualmente ou em associação, formulem regras de governança e boas práticas, implementando tais programas e respeitando:

a) comprometimento do controlador em adotar políticas que assegurem o cumprimento da Lei;

b) aplicabilidade a todo o conjunto de dados pessoais em seu poder;

c) adaptação a sua estrutura;

d) objetivo de estabelecer relação de confiança com o titular;

e) integração com sua estrutura geral de governança;

f) existência de um plano de respostas a incidentes de segurança da informação;

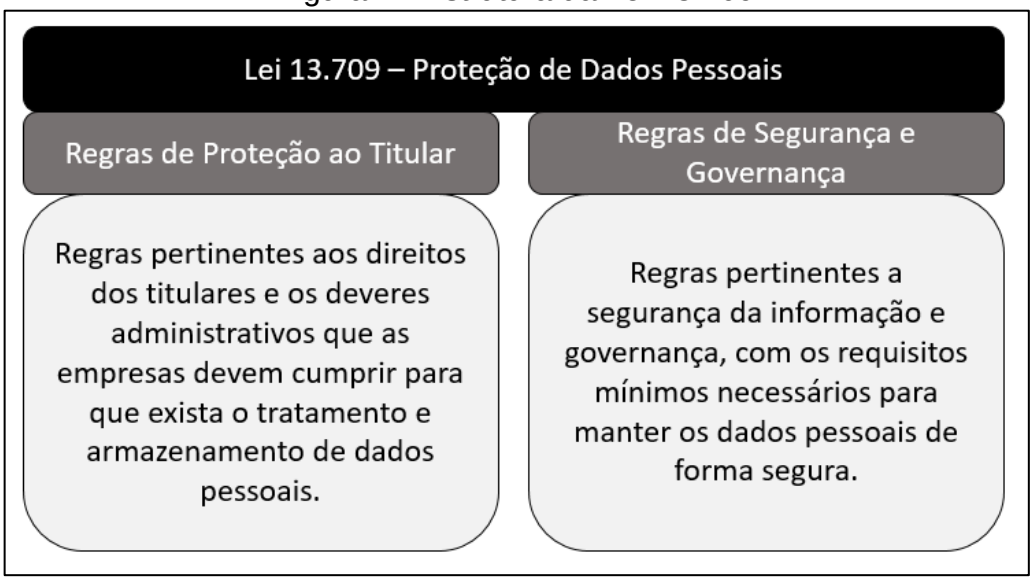
g) demonstrar efetividade em seu programa de governança.

2.8 CONSIDERAÇÕES FINAIS

A Lei Geral de Proteção de Dados estrutura-se de modo a fornecer regras no que diz respeito aos direitos dos cidadãos quando do fornecimento de dados pessoais para organizações ou entidades públicas ou privadas, bem como sobre os deveres e requisitos a serem cumpridos por estas em manter, de forma segura e em privacidade, qualquer tipo de dado pessoal que for necessário para realização de suas operações.

De forma geral, a Lei 13.709 pode ser dividida em dois grupos de regras. O primeiro, que pode ser chamado de Regras de Proteção ao Titular, disponibiliza as regras pertinentes a direitos dos titulares e os deveres administrativos que as organizações precisam cumprir para que os dados possam ser mantidos e tratados. O segundo, Regras de Segurança e Governança, apresenta regras pertinentes a segurança da informação e governança, com os requisitos mínimos necessários para manter os dados pessoais de forma segura. A Figura 2 mostra essa divisão de forma resumida.

Figura 2 - Estrutura da Lei 13.709



Fonte: Próprio autor.

O maior grupo, Regras de Proteção ao Titular, abrange as regras que visam a proteção da privacidade do cidadão. Primeiramente, são apresentadas as regras para que o titular explicite sua vontade em fornecer seus dados pessoais para tratamento, e como esse consentimento pode ocorrer. Além disso, também dispõe sobre as hipóteses em que o tratamento e armazenamento de dados pessoais pode acontecer sem o consentimento do titular. Inclui as informações que o responsável pelo tratamento dos dados deve disponibilizar, tanto aos titulares, como para a autoridade nacional e, também, para a população de forma geral. Estas informações incluem as finalidades do tratamento, como o tratamento é feito e o que deve acontecer após o tratamento dos dados. De uma maneira geral, são as regras para coleta, armazenamento, tratamento, alteração, manutenção e eliminação de dados pessoais que as empresas devem cumprir, visando a transparência e a garantia dos direitos de privacidade e individualidade dos titulares.

O segundo grupo, Regras de Segurança e Governança, apesar de menor, apresenta os requisitos mínimos para garantir que os dados em poder das organizações estejam seguros. Segundo a Lei, as organizações devem prover meios técnicos que evitem vazamentos de dados, acessos não autorizados, perda indevida de dados ou tratamento de forma não autorizada, além de garantir a transmissão segura dos mesmos, a sua disponibilidade e o devido gerenciamento dos meios adotados para manter a segurança destes. Os métodos que devem ser utilizados para

isso não são informados, mas a necessidade de adoção de meios de proteção deve ser observada em todos os processos em que os dados pessoais estejam envolvidos, o que inclui a coleta dos dados, os dispositivos de armazenamento, a infraestrutura envolvida, os sistemas utilizados para tratamento, segurança física dos ambientes em que os dados estão armazenados, bem como a gestão da segurança de todos os processos envolvidos. A Lei também apresenta a possibilidade da criação de normas e regras de boas práticas, no que diz respeito a políticas de governança. Essas normas devem estar em concordância com os requisitos da Lei, além de serem compatíveis com Políticas de Governança já adotadas pela organização.

Após um resumo do que trata a Lei 13.709, seus requisitos e uma abordagem inicial do que é necessário em termos técnicos para manter a segurança de dados pessoais em poder de organizações, é preciso apontar os mecanismos de segurança a ser adotados para atender a Lei, assunto que é abordado no Capítulo 3.

3 MECANISMOS, SISTEMAS E FERRAMENTAS DE SEGURANÇA DA INFORMAÇÃO

A informação em poder de organizações é um ativo de grande valor, e já vem sendo tratada dessa maneira há algum tempo. Portanto, a manutenção de sua segurança em uma organização é de grande importância, devendo ser mantida em proteção e bem gerenciada, dentro de um ambiente que também proporcione tal nível de controle. Segundo a norma ABNT NBR ISO/IEC 27002 (2005), “a segurança da informação é obtida através da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*”. De forma geral, a segurança da informação é o conjunto de práticas que busca eliminar ou reduzir ao máximo os fatores que venham a afetar um ou mais dos três princípios da segurança da informação, que são (OLIVEIRA, 2001; GOODRICH, TAMASSIA, 2013):

a) confidencialidade: consiste na garantia de que apenas pessoas ou entidades autorizadas tenham acesso à informação. A informação deve estar disponível somente a quem realmente necessita acessá-la, e esse princípio visa, portanto, o impedimento que esta seja violada, mantendo-a em sigilo;

b) integridade: é a garantia de que as informações armazenadas realmente estão corretas e são verdadeiras, mantendo a forma que foram coletadas ou foram atualizadas mediante autorizações pré-estabelecidas. Também visa garantir que as informações, quando enviadas de um ponto a outro, se mantenham intactas;

c) disponibilidade: garantia de que as informações estarão disponíveis sempre que solicitadas pelas pessoas autorizadas.

Com a aprovação da Lei de Proteção de Dados Pessoais, a manutenção de dados em segurança atinge um novo patamar, deixando de atender apenas os interesses particulares da organização. Devem existir meios que garantam, não apenas a segurança e inviolabilidade dos dados, mas também, que mantenham a privacidade dos titulares de dados pessoais em poder das organizações. A segurança, nesse contexto, envolve todos os processos da informação, desde o armazenamento, o tratamento, a transferência e a eliminação.

Para manter a segurança dos dados, conforme os requisitos da Lei, é necessário o conhecimento dos riscos e ameaças a que estes estão expostos. Dessa maneira, é possível indicar quais as medidas técnicas de segurança que as empresas devem adotar. Sendo assim, este capítulo trata das principais ameaças de segurança da informação relacionadas à proteção de dados pessoais, conforme a Lei 13.709 e os meios técnicos que podem ser adotados para manter estes dados em segurança, atendendo os requisitos propostos na Lei.

3.1 AMEAÇAS E MEIOS TÉCNICOS DE PROTEÇÃO DE DADOS

Conforme exposto no início deste capítulo, existem ameaças que podem corromper os princípios da segurança da informação. Ameaças são fatores que podem comprometer as informações, por meio da exploração de vulnerabilidades, provocando impactos aos negócios e à organização (SÊMOLA, 2003). Em resumo, é qualquer coisa ou situação que coloque em risco a informação armazenada, causando prejuízos a organização.

As vulnerabilidades são pontos fracos, que permitem que uma ameaça possa agir de forma a ocasionar um incidente de segurança (HINTZBERGEN, 2018), afetando um ou mais dos princípios de segurança da informação. Por si só, uma vulnerabilidade não consegue provocar um incidente, necessitando de um agente causador ou uma condição favorável para isso. O Quadro 1 exemplifica algumas vulnerabilidades existentes (SÊMOLA, 2003; ABNT NBR ISO/IEC 27005, 2008).

Quadro 1 - Exemplos de vulnerabilidade

(continua)

Tipo de vulnerabilidade	**Exemplo**
Físicas	Instalação predial fora de padrão, em local propício a desastres
	Data center mal projetado, incluindo falhas no fornecimento de serviços como energia elétrica
	Falhas em sistema de combate a incêndio
	Falta de controle de acesso físico às dependências da organização.
Hardware	Falha em recursos de TI ou erros em instalação de componentes.
	Manutenção insuficiente em mídias de armazenamento.

(continua)

Hardware	Sensibilidade à umidade, poeira, sujeira, radiação eletromagnética, variações de temperatura, variações de voltagem.
	Inexistência de uma rotina de substituição de equipamentos.
	Falta de cuidados no descarte de equipamentos.
	Realização de cópias não controladas.
Software	Erros na instalação, podendo acarretar em acessos indevidos, vazamento ou perda de dados ou indisponibilidade.
	Erros de configuração, podendo acarretar em acessos indevidos, vazamento ou perda de dados ou indisponibilidade.
	Falhas de testes ou instalação de softwares imaturos.
	Download ou uso de softwares sem controle.
	Inexistência de cópias de segurança.
	Falta de controle de serviços necessários para cada usuário.
	Atribuições errôneas de acesso a usuários.
	Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de usuários.
Mídia	Discos, fitas, relatórios impressos podem ser perdidos ou danificados.
	Descarte ou uso indevido de mídias sem a devida remoção dos dados.
	Acesso não monitorado / controlado a mídias de armazenamento.
Comunicação	Acessos não autorizados.
	Falta de registros de operações e tráfego de informações na rede.
	Tráfego de informações desprotegido.
	Cabeamento e estrutura mal projetados / instalados.
	Arquitetura de rede insegura.
	Senhas desprotegidas.
	Falta de autenticação e identificação em transmissões de dados.
	Perda de comunicação.
	Roubo de informação.
Humanas	Falta de treinamento em segurança da informação.
	Compartilhamento indevido de informações.
	Falha na execução de rotinas de segurança.

(conclusão)

Humanas	Trabalhos não supervisionados por terceiros ou fornecedores de serviço.
	Erros ou omissões em tarefas.
	Sabotagens.
	Vandalismo.
	Roubo.
	Destruição de propriedade.
	Invasões.
Organização	Falta de gerenciamento de segurança da informação.
	Falta de políticas de controle de acessos.
	Contratos com terceiros sem provisões de segurança da informação.
	Falta de auditorias de segurança.
	Inexistência de documentação relativa a Segurança da Informação.
	Atribuições inadequadas de responsabilidades pela segurança da informação.
	Inexistência de planos de contingência e recuperação de dados.
	Inexistência de mecanismos estabelecidos para o monitoramento de violações da segurança.

Fonte: Próprio autor.

O Quadro 2 apresenta exemplos de ameaças que podem pôr em risco os dados pessoais em poder de uma organização explorando vulnerabilidades existentes, conforme disponibilizado na literatura (OLIVEIRA, 2001; ABNT NBR ISO/IEC 27005, 2011; SÊMOLA, 2003).

Quadro 2 – Ameaças

(continua)

Tipos de Ameaça	**Definição**
Tratamento Ilegal dos Dados	Os dados são tratados de forma além do que foi consentido pelo titular, ou para outros fins que não foram previamente definidos pela organização.
Divulgação Indevida	Os dados são tratados e divulgados sem autorização do titular.
Cópia Ilegal	Os dados são copiados para outro ponto de armazenamento que não o estipulado pelo controlador ou consentido pelo titular, de forma ilegal.
Espionagem Interna e Externa	Ato ou efeito de espionar, podendo ser de pessoas de fora ou de dentro da empresa.

(continuação)

Dano físico à mídia	Quando o dispositivo ou mídia sofre alguma ação de prejuízo, acidental ou intencional, ocasionando a perda dos dados e da mídia.
Engenharia Social	Manipulação psicológica de pessoas para a execução de ações ou divulgação dos dados privados.
Modificação de dados sem autorização	Os dados são alterados / modificados sem autorização do titular.
Ataques baseados em senhas	Um software malicioso realiza a execução de algoritmos baseados em dicionários de palavras na tentativa de descobrir a senha original, com intuito de acessar ilegalmente os dados armazenados ou ter acesso indevido às informações em poder do controlador.
Acesso não autorizado	Os dados são acessados por pessoas sem a devida permissão.
Abuso de poder	Membro da organização com posição hierárquica maior utiliza-se de sua autoridade para obter acesso indevido aos dados armazenados.
Comprometimento dos dados	Os dados sofrem algum tipo de incidente, ocasionando a perda de integridade da informação armazenada.
Acesso a links de fontes não conhecidas ou não confiáveis	Acesso a links ou *sites* com fonte desconhecida, que podem apresentar ameaças ou conteúdo malicioso que, porventura, possam causar prejuízos à integridade e privacidade dos dados armazenados.
Furto de equipamentos	Roubo dos equipamentos da organização, tornando as informações dos dispositivos indisponíveis ou vulneráveis a acessos indevidos.
Uso não autorizado do equipamento	O equipamento é utilizado por pessoas sem autorização.
Falhas de protocolo	Alguma falha de comunicação entre os protocolos, deixando os dados vulneráveis a interceptação.
Exploração de vulnerabilidade	Falhas de processo que, quando exploradas, resultam na violação da segurança dos dados.
Falhas de Autenticação	O sistema possui erros de projetos, levando a falhas de autenticação e possíveis acessos indevidos a dados confidenciais.
Software Malicioso	Qualquer software indesejado, instalado sem autorização, deixando os dados vulneráveis a acessos ou ações indevidas.
DDoS / DOS- Ataques de Negação de Serviço	Ataques que visam causar indisponibilidade dos serviços de um determinado processo, através do envio de simultâneas requisições.

(conclusão)

Interceptação de dados	Ato de interceptar uma transmissão de dados que estiver sendo feita de forma insegura, podendo haver acesso ilegal ou indevido aos dados.

Fonte: Próprio autor.

3.2 MEDIDAS DE SEGURANÇA

Medidas de segurança são as práticas, os procedimentos e os mecanismos usados para a proteção da informação. Este conjunto de controles tem por objetivo reduzir os riscos de ocorrência de um incidente a um nível aceitável, o qual deve ser definido pela organização, com base em suas políticas e objetivos, como também atendendo a legislações e regulamentações relevantes (ABNT NBR ISO/IEC 27002, 2005).

As medidas de segurança a serem adotadas podem ser classificadas de três formas (SÊMOLA, 2003): preventivas, detectáveis ou corretivas. As medidas preventivas são aquelas que objetivam evitar o acontecimento de incidentes. Medidas detectáveis visam identificar condições ou indivíduos causadores de ameaças, com o intuito de evitar que estas explorem vulnerabilidades existentes. Já as medidas corretivas são ações que resultam na correção de uma estrutura, visando a retomada de uma condição normal de operação após o acontecimento de um incidente.

O Quadro 3 apresenta as principais medidas de segurança encontradas na literatura (KUROSE, ROSS, 2013; OLIVEIRA, 2001; FONTES, 2006; TANENBAUM, WETHERALL, 2011; GALVÃO, 2015; GOODRICH, TAMASSIA, 2013).

Quadro 3 - Medidas de segurança

(continua)

Medida de segurança	**Descrição**
Criptografia	Técnica que transforma uma mensagem em outra, de forma a “esconder” a mensagem original, com a criação de uma chave para reverter para a mensagem original.
Firewall	Sistema que isola a rede interna de uma organização da Internet, permitindo que alguns pacotes passem, e bloqueando outros (geralmente possíveis ameaças).
Sistema de detecção de invasão	Dispositivo que gera alertas de pacotes mal-intencionados que pretendem adentrar a rede interna de uma organização.

(continuação)

Antivírus	Aplicativos instalados em computadores com a finalidade de proteger estes de ataques de programas de vírus.
Proteção de e-mail	Sistemas de segurança que fornecem proteção no trânsito de mensagens entre dois *sites* distintos.
Autenticação	Processo em que uma entidade prova sua identidade a outra em uma rede de computadores.
Controles de acesso	Recurso utilizado para definir e limitar ações que usuários, aplicativos ou programas podem realizar nos dados armazenados.
Virtual Private Network (VPN)	Tecnologia que permite transmissão segura de dados entre dois pontos específicos, utilizando protocolos de segurança, através de redes públicas, como a Internet.
Security Socket Layer (SSL)	Protocolo implementado em servidores e browsers, garantindo o tráfego seguro de dados na internet.
IPv6	Protocolo de endereçamento de pacotes de dados na Internet, com o objetivo de garantir o envio para o destinatário corretamente, pelo melhor caminho.
Gerenciamento de redes	Implantação de ferramentas adequadas para monitorar, gerenciar e controlar a rede, com o objetivo de manter a plena operação da mesma.
Proxy Systems	Implementação de um serviço que atua como filtro entre cliente e servidor, não permitindo que eles se comuniquem diretamente e provendo apenas as operações necessárias para fornecer o serviço.
Anti-*Malware*	Sistemas e práticas adotados para evitar ataques ou incidentes causados por programas ou elementos mal-intencionados.
Autenticação digital e certificação digital	Método de identificação e autenticação de usuários, utilizando um elemento digital confiável, assegurado por uma entidade certificadora com mesma validade jurídica de um cartório tradicional.
Segurança física a informação	Uso de medidas físicas para proteção de equipamentos e recursos que contenham informações e dados.
Cópias de segurança	Procedimentos adotados para duplicação de dados, de forma segura, permitindo sua recuperação no caso da ocorrência de um incidente.
Plano de continuidade	Adoção de políticas que definam ações para garantir a operação da organização no caso de ocorrência de um incidente.

(conclusão)

Gestão da Segurança da Informação	Conjunto de políticas, regras e processos implantados para garantir a Segurança da Informação de forma ampla em uma organização.

Fonte: Próprio autor.

3.3 MEDIDAS DE SEGURANÇA NECESSÁRIAS À LEI 13.709

Analisando a Lei 13.709, é possível dividir as necessidades de medidas de Segurança da Informação conforme segue:

a) transmissão segura dos dados;

b) controle de acessos aos dados;

c) proteção contra vazamentos de dados;

d) proteção à integridade dos dados;

e) proteção quanto à perda indevida dos dados;

f) garantia da disponibilidade dos dados;

g) gerenciamento da segurança dos dados.

Para cada um dos pontos dispostos acima, existem ameaças específicas e medidas de segurança que devem ser implantadas ou adotadas, a fim de reduzir os riscos de ocorrência de incidentes que venham a violar os requisitos da Lei. Estas medidas serão apresentadas nas seções que seguem, conforme cada necessidade imposta pela Lei.

3.3.1 Transmissão segura dos dados

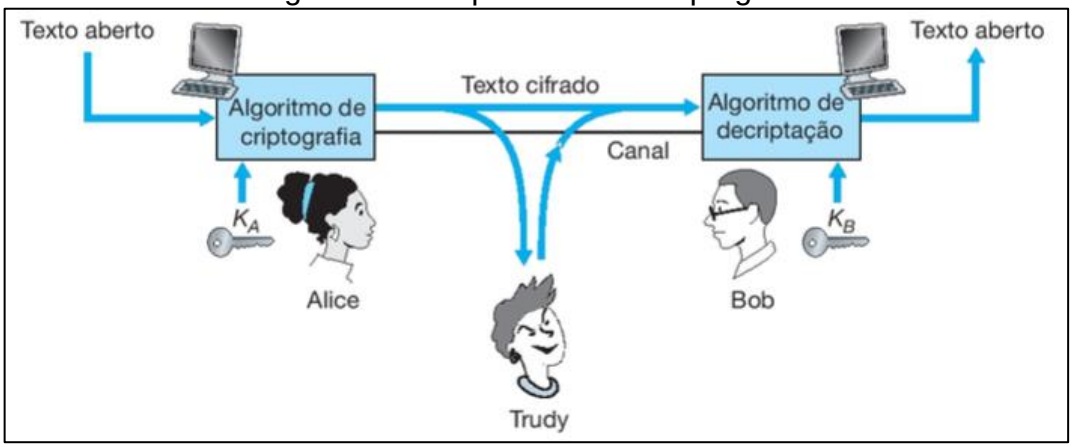
Conforme disposto na Lei, o titular dos dados tem o direito de obter informações quanto aos dados em poder de uma organização, bem como os próprios dados de forma integral. Também existe a possibilidade de se compartilhar os dados entre organizações ou a transmissão dos mesmos para fora do país. Além disso, uma organização que possui dados pessoais em seu poder pode possuir mais de um local de armazenamento para os mesmos, existindo a necessidade de transferir dados de um ponto para outro em algum momento. Em qualquer uma dessas situações, existe a necessidade de que os dados em trânsito estejam seguros, com a adoção das devidas medidas para garantir isto.

Durante o processo de transmissão de dados, pode ocorrer uma interceptação dos mesmos, que, por sua vez, pode acarretar em uma cópia de forma ilegal ou divulgação indevida dos dados pessoais. A interceptação ocorre através da exploração de vulnerabilidades de segurança em rede ou em protocolos de comunicação. A falta de barreiras de segurança em uma mensagem em trânsito permite que ela seja acessada enquanto trafega na rede ou Internet, ou pode existir a possibilidade que ela seja recebida por uma pessoa ou entidade mal-intencionada. Mesmo que os dados sejam recebidos pelo destinatário correto, ela pode ter sido acessada por um intruso durante sua transmissão, sem que se perceba explicitamente que isto ocorreu.

Para evitar que dados em trânsito sejam suscetíveis a interceptação ou cópia de dados de forma ilegal, devem ser adotadas medidas como criptografia dos dados enviados, utilização de protocolos seguros de comunicação, como o IPv6, ou a utilização de canais seguros de transmissão, como uma VPN.

A criptografia dos dados consiste em cifrar uma mensagem no remetente, manter ela cifrada durante a transmissão, e decifrar quando chega ao destinatário. Para evitar que qualquer pessoa receba a mensagem cifrada e possa decifrá-la, são utilizadas chaves, que são códigos (como senhas) que permitem que autorizam a decriptação, desde que sejam corretas. A Figura 3 mostra como ocorre a transmissão de mensagens com criptografia. Alice envia uma mensagem criptografada para Bob, utilizando a chave de criptografia *K*. Trudy, por sua vez, intercepta a mensagem no caminho, mas não consegue visualizar a mesma por não possuir uma chave de decriptação.

Figura 3 - Componentes de criptografia



Fonte: Kurose, Ross, 2013.

Existem dois grupos de criptografia: de chave única ou simétrica e de chaves públicas ou assimétricas. O sistema de chave única utiliza a mesma chave para criptografar e decriptografar a mensagem, portanto, o remetente e o destinatário devem possuir a mesma chave. O sistema de chaves públicas apresenta uma arquitetura que utiliza, além da chave privada do remetente e do destinatário, uma chave pública disponível para ambos. Para enviar uma mensagem, o remetente busca a chave pública do destinatário, que está disponível para todo mundo. A criptografia da mensagem é feita utilizando esta chave pública. Ao receber a mensagem criptografada, o destinatário utiliza a sua chave pública (disponível para todos), juntamente com sua chave privada para efetuar a decriptação da mesma. É um método mais seguro, porém, mais lento que uma criptografia de chave única. Os processos de criptografia compreendem algoritmos complexos, que podem ser melhor compreendidos analisando bibliografia pertinente, como em Carissimi, Rochol e Zambenedetti (2009), Kurose, Ross (2013) e Goodrich, Tamassia (2013).

A utilização de criptografia não impede que a mensagem possa ser interceptada por alguém mal-intencionado, mas dificulta bastante a interpretação da mesma. E, justamente, é este o objetivo da utilização desta técnica. Manter os dados protegidos enquanto estão em trânsito, mesmo que estes sejam interceptados por um intruso durante o processo.

A transmissão segura de mensagens também pode utilizar o protocolo de comunicação IPv6. O protocolo IP é o padrão utilizado para definir o conteúdo de cada pacote de dados que trafega na Internet. Em sua versão de número 6, o protocolo IP traz implementações que garantem uma forma mais segura de envio de dados (KUROSSE, ROSS, 2013; CARISSIMI, ROCHOL, ZAMBENEDETTI, 2009). Um exemplo é a utilização do mecanismo *Authentication Header* (AH). Neste método, o cabeçalho dos pacotes enviados possui autenticação, garantindo a identidade do remetente e que os pacotes não foram alterados durante a transmissão. Outro método que pode ser utilizado é o mecanismo *Encrypted Security Payload* (ESP), que garante a privacidade dos dados ao criptografar os dados enviados, armazenando as informações em um cabeçalho ESP. Este método possibilita que os dados não sejam compreendidos caso sejam interceptados por um intruso. A utilização dos dois métodos é possível com a implementação de cabeçalhos de extensão no protocolo

IPv6. Estes cabeçalhos contêm informações adicionais ao cabeçalho principal de um pacote de dados transmitidos.

A utilização de uma Rede Virtual Privada (*Virtual Private Networking,* VPN) também é um método válido para evitar a interceptação de dados em uma transmissão. Esse método consiste em criar uma rede privada entre dois pontos distantes, utilizando uma rede pública, como a Internet, como meio de transporte (GOODRICH, TAMASSIA, 2013). A utilização desse método garante confidencialidade, integridade e autenticação de dados. Não existe um padrão único para redes VPN, cabendo a cada empresa de comunicação oferecer, de forma competitiva, soluções conforme sua estrutura permite. Redes VPN utilizam mais de um protocolo de comunicação, aproveitando suas características de segurança, para criar uma espécie de túnel entre os dois pontos que necessitam conexão (GOODRICH, TAMASSIA, 2013). Esse conjunto de protocolos é utilizado, por vezes, com implementação de IPsec[2], assegurando autenticação, integridade e confidencialidade. Dessa forma, se uma empresa deseja enviar dados pessoais entre dois pontos distantes (em um compartilhamento de dados com outra empresa, ou entre duas filiais situadas em locais fisicamente distantes, por exemplo), os mesmos estão protegidos contra acessos indevidos ou interceptações em trânsito.

Outra ameaça que pode corromper a segurança de dados em trânsito é a ocorrência de falhas em protocolos de comunicação. A implementação de protocolos mais atuais, com a utilização dos métodos de segurança que estes proporcionam, é uma alternativa para manter os dados seguros em transferências utilizando redes públicas. O protocolo IPv6, apresentado anteriormente nesta seção, é a última versão do protocolo IP, utilizado para coordenar os pacotes de dado que são enviados de um ponto a outro (KUROSE, ROSS, 2013). Erros que ocorriam em versões mais antigas, como IPv4, foram corrigidos nessa versão, além da ampliação de opções de segurança para transmissão de dados.

[2] IPsec é um protocolo IP de segurança, utilizado em redes VPN como um adicional aos pacotes IP padrões de comunicação (IPv4 e IPv6). Durante o trânsito do pacote pela Internet, ele é visto como um pacote padrão de dados, utilizando os cabeçalhos IPv4 e IPv6. Porém, esses pacotes carregam em seu conteúdo um pacote IPsec, que, por sua vez, carrega os dados de forma criptografada. O protocolo IPsec garante que os dados sejam decifrados somente pelo destinatário correto, que os dados sejam recebidos de forma integra, e possibilitam a autenticação dos usuários envolvidos.

A interceptação de dados, onde um intruso obtém acesso de forma ilegal aos dados em trânsito, pode ser evitada utilizando medidas apresentadas anteriormente nesta seção, as quais são: criptografia, VPNs e protocolos de comunicação atuais, como IPv6. Além desses recursos, que evitam que os dados sejam compreendidos por entidades não autorizadas, existe também medidas para implementação de proteção de e-mail. Uma vez que exista a necessidade de envio de dados pessoais com a utilização de e-mails, é necessário que esta transmissão seja imune a interceptação por indivíduos não autorizados. Uma proposta de proteção de e-mail é a utilização de métodos já apresentados nessa seção, como autenticação e criptografia. Em 1991, um esquema de criptografia foi desenvolvido exclusivamente para e-mails (KUROSE, ROSS, 2013), denominado *Pretty Good Privacy* (PGP). O PGP é um padrão bastante utilizado atualmente, existindo algumas versões públicas e sua implementação em diversas plataformas de envio de mensagens. Consiste, basicamente, em um sistema que utiliza chaves públicas e privadas para proteger o conteúdo das mensagens, juntamente com a inclusão de assinatura digital à estas, já implementadas a uma plataforma de envio e recebimento de e-mails. Dessa maneira, as informações enviadas mantêm preservadas sua integridade e sua privacidade.

O Quadro 4 apresenta as ameaças que podem afetar os dados em trânsito, e as medidas de segurança a serem adotadas para dificultar ou evitar incidentes ou a violação da segurança dos dados.

Quadro 4 - Ameaças e medidas de segurança para transmissão segura de dados

Ameaça	**Medida de segurança**
Cópia ilegal de dados	Criptografia
	VPN
	IPv6
Acesso não autorizado	Criptografia
	VPN
Falhas de protocolo	IPv6
Interceptação dos dados	Criptografia
	VPN
	IPv6
	Proteção de e-mail

Fonte: Próprio autor.

3.3.2 Controles de acesso

A Lei 13.709 tem como premissa a garantia da privacidade dos dados pessoais em poder de uma organização ou entidade. Dentro desse conceito, os dados devem estar disponíveis apenas a quem realmente fará uso dos mesmos, e a necessidade do controle de quem acessa a informação é de grande importância. Esse controle não se resume apenas ao disco ou servidor onde os dados se encontram, mas engloba a área física onde se encontram os dados, além de todo o controle que é necessário a uso de redes em que os dados podem ser acessados de alguma forma.

Os dados pessoais devem ser visualizados e manipulados exclusivamente por pessoas autorizadas. O acesso livre a tais dados configura uma vulnerabilidade que expõe os mesmos a possíveis ataques, desrespeitando os requisitos da Lei e o princípio da privacidade em segurança da informação. Portanto, medidas devem ser adotadas para garantir que os dados estejam disponíveis somente para quem realmente deve utilizá-los, de qualquer forma.

O controle de acesso tem por objetivo evitar que pessoas ou entidades não autorizadas visualizem ou editem os dados, causando comprometimento à organização (GALVÃO, 2015). Também previne que ocorra o roubo de informações confidenciais. As regras para tal controle devem levar em consideração o modelo de segurança adotado pela empresa, além de legislação e normas vigentes.

A norma NBR ISO/IEC 27002:2005 possui uma seção que trata dos requisitos para controle de acessos (ABNT, 2005, p. 65-83), categorizando as mesmas conforme descrito no Quadro 5.

Quadro 5 - Categorias de controle de acessos

(continua)

Categoria	Objetivo
Requisitos de negócio para controle de acesso	Controlar o acesso à informação. Convém que o acesso à informação seja controlado com base nos requisitos de negócio e segurança da informação.
Gerenciamento do acesso do usuário	Assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação.
Responsabilidade dos usuários	Prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou furto da informação dos recursos de processamento da informação.

(conclusão)

Controle de acesso à rede	Prevenir acesso não autorizado aos serviços de rede.
Controle de acesso ao sistema operacional	Prevenir acesso não autorizado aos sistemas operacionais.
Controle de acesso à aplicação e à informação	Prevenir acesso não autorizado à informação contida nos sistemas de aplicação.
Computação móvel e trabalho remoto	Garantir a segurança da informação quando se utilizam a computação móvel e recursos de trabalho remoto.

Fonte: Próprio autor.

Além dos controles apresentados no Quadro 5, também são necessárias medidas que venham a controlar o perímetro onde os dados ficam armazenados. A proteção física tem como objetivo evitar o furto dos dados através do acesso aos meios físicos onde estes estão armazenados, como discos rígidos, servidores, mídias de armazenamento, fitas ou cópias de backup, computadores e outros equipamentos que tenham algum tipo de dado armazenado.

O controle de acesso parte da definição de quem pode ou não ter acesso aos dados, e até onde esse acesso é permitido. Existem usuários que não tem privilégios de alteração de alguns dados, podendo somente visualizá-los. É essencial que a organização, ao criar meios de controle de acesso, tenha uma política de controle de acesso estabelecida e documentada, tendo como base os requisitos de acesso do negócio e segurança da informação (ABNT, 2013). Essa política deve partir da premissa mais segura de que tudo é proibido, a menos que expressamente permitido.

A política de controle de acesso deve conter as autorizações de cada usuário aos sistemas de informação, além de informar os privilégios de acesso a cada um dos produtos de sistema, como sistema de gestão, sistemas operacionais e bancos de dados. Cada usuário deve estar ciente de suas permissões de acesso e dos requisitos de negócio que devem ser cumpridos com a utilização dessas permissões. A política de controle de acesso, por sua vez, deve ser analisada periodicamente, eliminando ou adicionando acessos conforme as necessidades da organização, respeitando

requisitos da legislação e normas pertinentes. Além disso, a política de controle de acesso deve prover meios de responsabilização dos usuários quanto às suas práticas na utilização de acessos permitidos.

Com uma política de acessos estruturada, é necessário utilizar ferramentas e mecanismos que proporcionem o seu atendimento. Um desses artefatos é o conjunto de mecanismos de autenticação e autorização. A adoção desses mecanismos é destinada a suprir os processos de identificação de pessoas, equipamentos, sistemas e agentes em geral (SÊMOLA, 2003). Sem que exista essa identificação, fica praticamente impossível realizar o controle de acesso aos sistemas de informação. Os métodos de identificação são divididos em três grupos (GALVÃO, 2015):

a) o que você sabe: método largamente utilizado pela sua facilidade de implantação. Consiste na utilização de alguma informação que somente o indivíduo saiba, como senhas ou PIN (*Personal Identification Number*). É um método vulnerável a falhas, pois depende da responsabilidade do indivíduo em não divulgar sua senha para outras pessoas, ou utilizá-la de forma indevida. Além disso, deve ser considerada a proposta de criação de senhas fortes (com maior dificuldade de serem descobertas), evitando a utilização de termos que representem informações do mundo real, como placas de veículos, datas de nascimento ou nomes de parentes. Outro ponto que deve ser considerado é a substituição das senhas em intervalos definidos de tempo, como maneira de dificultar sua identificação por outras pessoas que não seus proprietários. A utilização deste método compreende grande parte dos acessos necessários em um sistema de informações, como acesso à rede, a sistemas operacionais, a bancos de dados ou, até mesmo, a meios físicos, o qual será exposto posteriormente nesta seção;

b) o que você tem: método que utiliza dispositivos físicos para autenticação de acessos. Existem vários mecanismos que se encaixam nesse conjunto. A escolha de qual utilizar depende do nível de segurança necessário e do orçamento disponível para implantação. Como exemplos, podem ser citados cartões com códigos de barras, cartões magnéticos e *tokens*.

c) o que você é: método de autenticação que utiliza métricas biométricas para identificar pessoas que desejam acessar algum sistema. Seu custo ainda é

> elevado, comparado aos outros métodos citados anteriormente, mas sua utilização está se popularizando, como, por exemplo, na autenticação de utilização de *smartphones* que utilizam leitura de impressões digitais para desbloqueio. É um método bastante seguro, uma vez que utiliza informações do corpo humano e que são únicas para cada indivíduo. Como exemplos, podem ser citados leitura de impressões digitais, leitura de geometria da face, leitura de geometria das mãos, reconhecimento de voz e leitura de íris.

Os métodos expostos anteriormente são utilizados para acesso aos sistemas de informação de forma geral. Além deste ponto de controle, é necessário que os responsáveis pela aplicação das políticas de acesso discriminem os privilégios de acesso de cada entidade ou usuário. Os privilégios compreendem até onde o acesso concedido pode ser explorado. Em outras palavras, define o que o usuário pode ou não pode fazer após o acesso aos sistemas de informação. Isso garante que somente quem possui atribuições de alteração ou manipulação dos dados possa assim fazer, evitando que os dados sejam excluídos ou modificados de forma indevida.

Também é aconselhável manter registros de acessos a banco de dados e sistemas de informação, bem como registros das atividades efetuadas. Dessa forma, o controle das atividades de cada usuário fica evidente, auxiliando na análise das políticas de acessos, bem como na detecção de alguma atividade efetuada de maneira incorreta, auxiliando em soluções de contorno.

Os meios físicos de armazenamento de dados também devem possui controles de acesso. Servidores e bancos de dados, mídias ou discos de armazenamento não devem ficar acessíveis a qualquer indivíduo dentro de uma organização. O livre acesso expõe equipamentos que possam conter dados pessoais, possibilitando vazamentos de dados ou roubo de informações de forma ilegal. Segundo a Norma NBR ISO/IEC 27002 (ABNT, 2013), é conveniente que sistemas sensíveis à organização sejam mantidos em ambiente isolado e dedicado. Como medidas de controle de acessos físicos podem ser citados os controles de acesso à organização, controles específicos de acesso para departamentos da organização, trancas com dispositivos que limitem o acesso a salas e cofres, construção que permita manter equipamentos de informação sem livre acesso de pessoal, além de controles de vigilância, como câmeras ou alarmes de intrusão.

Os dispositivos móveis, como *notebooks* e *smartphones*, por exemplo, também devem estar incluídos nas políticas de controles de acessos (ABNT, 2013). A utilização destes aparelhos deve ser controlada, e, quando permitido o acesso aos sistemas de informação por meio dos mesmos, os privilégios devem ser muito bem definidos, uma vez que a facilidade com que dados e informações podem ser copiados e extraídos do ambiente organizacional é bem grande.

De forma geral, o Quadro 6 apresenta algumas das medidas de controle de acesso que podem ser utilizadas, conforme literatura (SÊMOLA, 2003; GOODRICH, TAMASSIA, 2013; GALVÃO, 2015).

Quadro 6 - Exemplos de controles de acessos

	Tipo de acesso	**Exemplo de controle**
Acessos físicos	Acessos a organização	Controle de acesso de visitantes.
		Controle de acesso de funcionários.
Acessos físicos	Acessos a departamentos	Catracas de controle de acesso físico.
		Trancas com utilização de dispositivos de acesso, como senhas, cartões magnéticos ou biometria.
		Circuitos internos de monitoramento de imagem.
	Estrutura predial	Salas cofre para instalação de servidores e dispositivos de armazenamento e processamento de informação, com controles e monitoramento de acessos.
		Circuitos internos de monitoramento de imagem.
		Alarmes de intrusão.
Acessos lógicos	Senhas, *PIN*	Controle de acesso a sistemas baseado em algo que o indivíduo saiba.
	Cartões de acesso, *Tokens*	Controle de acesso a sistemas baseado em algo que o indivíduo possua.
	Leitor de impressão digital, geometria da face, reconhecimento de voz, leitor de íris	Controle de acesso a sistemas baseado em algo que o indivíduo é, baseado em informações do seu corpo.

Fonte: Próprio autor.

De forma geral, o controle de acessos parte da elaboração de uma política bem definida, esclarecendo de forma minuciosa quem pode acessar e o que pode acessar dentro dos sistemas de informação dentro da organização e, consequentemente,

dados pessoais armazenados ou em tratamento. Os controles adotados para tal partem destas políticas, que devem ser divulgadas aos usuários e estes devem estar cientes de suas responsabilidades quanto ao cumprimento das normas estabelecidas na empresa. O Quadro 7 apresenta as ameaças correspondentes a acessos de dados, e quais os controles a serem adotados para evitar incidentes.

Quadro 7 - Ameaças e medidas de segurança para acessos aos dados

Ameaça	**Medidas de segurança**
Cópia ilegal	Política de controles de acessos
	Controles de acessos lógicos
	Controles de acessos físicos
Modificação de dados sem autorização	Política de controles de acessos
	Controles de acessos lógicos
Acesso não autorizado	Política de controles de acessos
	Controles de acessos lógicos
Furto de equipamentos	Política de controles de acessos
	Controles de acessos físicos
Uso não autorizado de equipamentos	Política de controles de acessos
	Controles de acessos lógicos
	Controles de acessos físicos

Fonte: Próprio autor.

3.3.3 Armazenamento seguro dos dados

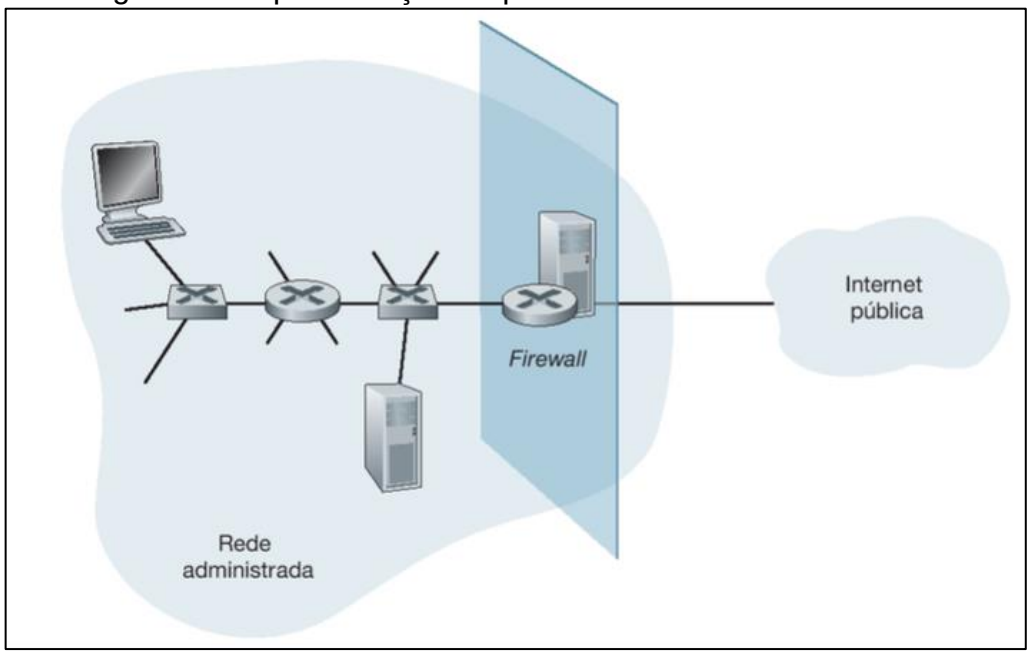
A Lei 13.709 não requisita explicitamente que os dados devem ser armazenados de forma segura, porém, isto é necessário para cumprir com outros requisitos envolvidos. Devem existir barreiras que evitem ataques de segurança aos dados armazenados em poder de organizações, impedindo que os mesmos sejam acessados de forma ilegal ou indevida, sejam corrompidos ou perdidos de forma não autorizada, sejam copiados por indivíduos mal-intencionados ou, até mesmo, espionados, tendo sua privacidade violada.

Uma das barreiras necessárias para manter a segurança do armazenamento é o controle de acessos à informação, exposto na seção 3.2.2 – Controles de acessos. Além disso, são necessárias medidas para manter todo o sistema de informações inerte a ameaças, com a utilização de controles que dificultem ou não permitam ataques de intrusão, bem como detectem no menor tempo possível quando um incidente de intrusão aos sistemas de informação ocorrer.

Primeiramente, deve existir uma política formal que defina a maneira com que os sistemas de informação devem ser utilizados e as responsabilidades e limites impostos a cada usuário (ABNT, 2013). A política de controle de acessos, apresentada na seção 3.3.2 deste trabalho, define os privilégios de cada usuário que tenha acesso aos sistemas. Ao definir tais privilégios, convém proibir a instalação de *softwares* em computadores e dispositivos conectados à rede da organização pelos usuários. Vírus ou códigos maliciosos podem estar disfarçados em arquivos de *softwares* e, se sua instalação não for controlada ou monitorada, os dados em poder da organização podem estar ameaçados, uma vez que estes códigos maliciosos podem roubar senhas e outras informações que venham a permitir um acesso mal-intencionado aos sistemas de informação (FONTES, 2006; OLIVEIRA, 2001). Também deve ser considerada a utilização de práticas como não permitir o uso de mídias removíveis em computadores (*pen-drives*, cartões de memória, CDs e DVDs), criar perfis de usuários em computadores com o mínimo possível de privilégios de acesso a configurações e instalação de programas ou desligar a auto execução de programas em computadores (GOODRICH, TAMASSIA, 2013).

A implementação de ferramentas de *Firewall* monta uma barreira entre a rede interna de uma organização e o mundo exterior (*Internet*). É uma combinação de *hardware* e *software* que atua como um filtro de pacotes, permitindo que alguns pacotes passem e outros não, dependendo da configuração executada pelos administradores de rede. Assim, definidas as políticas de segurança da organização, a utilização dessa medida permite controlar todo o tráfego de dentro para fora da empresa e vice-e-versa. Os pacotes que não possuírem permissão para passar pelo *Firewall* são descartados. Isso ajuda a prevenir o acesso a *sites* ou fontes indevidas pelo pessoal da organização, que, muitas vezes, faz isso sem ter conhecimento das possíveis ameaças, bem como também previne o acesso de pacotes com códigos maliciosos para a rede interna da organização (KUROSSE, ROSS, 2013; TANENBAUM, WETHERALL, 2011). A Figura 4 mostra como um *Firewall* pode ser posicionado entre a rede interna e a *Internet* em uma organização.

Figura 4 - Representação do posicionamento de um *Firewall*



Fonte: Kurosse, Ross (2013).

Outra medida que pode ser utilizada é a implementação de serviços de *proxy.* Um *Proxy System* atua como uma entidade intermediária entre o cliente e o servidor, verificando se as solicitações enviadas são válidas e, só então, estabelece a conexão com o servidor desejado fora da rede em que está instalado, e evitando uma conexão direta entre o cliente (usuário) e um servidor fora da rede da empresa. Opera em conjunto com o *Firewall*, acrescentando um nível de segurança a mais para a informação em poder da organização (OLIVEIRA, 2001). O serviço de *proxy* funciona como um procurador dentro da rede. Ele recebe a solicitação do cliente, verifica a validade da mesma e, se estiver coerente com as regras estipuladas, efetua a conexão com o serviço solicitado. Esta conexão é estabelecida entre o *proxy* e o servidor, não permitindo que o cliente entre em conexão diretamente com o serviço. Se o retorno do servidor for válido, conforme as regras configuradas no *proxy,* este recebe os dados e, então, estabelece uma conexão com o cliente para responder ao que foi solicitado. Esta medida, além de um filtro entre o usuário e o mundo externo à organização, também pode gerar um registro bem detalhado das operações efetuadas entre a rede interna e a *Internet*, permitindo um controle do que pode ou não entrar na rede da organização e as conexões que foram efetuadas pela mesma. Para a segurança dos dados armazenados na empresa, existe aqui um controle de acessos que, se bem configurado, pode proibir conexões com *sites* ou servidores que configurem ameaças a estes dados.

Uma medida para manter a segurança dos sistemas de informação conectados à rede da organização é a utilização de um sistema de detecção de invasão – IDS (*Intrusion detection system*). Este sistema verifica os pacotes que entram na rede da organização, comparando com um banco de dados de assinaturas de pacotes que representam algum tipo de ameaça aos sistemas de informação. Quando um ou mais pacotes suspeitos são recebidos, esses são bloqueados e um alerta é emitido aos administradores da rede, os quais podem, então, tomar as ações necessárias (KUROSE, ROSS, 2013). Os principais tipos de ameaça que este sistema pode detectar são: mapeamento indevido de rede, varreduras de portas não seguras, ataques de *DoS* (negação de serviço), vírus e *malwares*. Essa medida evita que indivíduos mal-intencionados possam adentrar a rede da organização com instalação de códigos malicioso, a fim de explorar vulnerabilidades existentes que permitam acesso aos dados de forma ilegal.

Também convém que sejam instalados programas antivírus e *anti-malware* nos computadores, dispositivos e servidores que os suportem dentro da organização (KIM; SOLOMON, 2014). Esses programas utilizam dados atualizados constantemente através dos servidores de seus desenvolvedores e que contém as informações das ameaças que podem afetar um computador ou sistema operacional, explorando vulnerabilidades que podem colocar em risco a privacidade dos dados armazenados. Através deste banco de dados, os programas antivírus e *anti-malware* podem impedir a entrada de um código malicioso em um sistema, como também permitem fazer uma varredura para verificar se algum destes códigos não está presente no dispositivo, o eliminando ou colocando em quarentena. Se todas as outras medidas de segurança vierem a falhar, permitindo que um vírus ou *malware* tente ser instalado em um computador, um antivírus pode garantir que não aconteça um incidente de segurança que signifique um risco aos dados pessoais em poder da organização.

Além de medidas técnicas, a implementação de uma política de segurança da informação na organização é de grande importância, pois é através dela que as boas práticas de utilização dos sistemas de informação são regradas. Segundo a Norma NBR ISO/IEC 27001 (2013), um Sistema de Gestão da Segurança da Informação (SGSI) é projetado para, além de outras atribuições, assegurar a seleção de controles de segurança necessários e adequados para proteger os ativos de informação de uma organização, onde se enquadram dados pessoais em poder desta. Maiores detalhes

sobre SGSI podem ser conferidos na seção 3.3.6 deste trabalho. Assim, a escolha e o regramento das ferramentas de segurança da organização dependem deste planejamento prévio, que deve ser definido conforme os objetivos da organização, respeitando requisitos de normas e legislativos, e ser divulgado e entendido por todos os envolvidos.

Por último, medidas tentando minimizar ataques de engenharia social devem ser implementadas. Ataques de engenharia social são aqueles onde indivíduos se fazem passar por outra pessoa ou personalidade, a fim de obter informações sigilosas e confidenciais, conquistando a confiança das pessoas (GALVÃO, 2015; FONTES, 2006). O treinamento constante de funcionários e colaboradores, além da divulgação das políticas de segurança e regras que devem ser respeitadas é a única maneira de tentar evitar este tipo de ataque a uma organização, diminuindo o risco de dados pessoais serem divulgados ou vazarem de forma ilegal.

Em resumo, os métodos para manter o armazenamento seguro dos dados pessoais em poder de uma organização estão representados no Quadro 8.

Quadro 8 - Ameaças e medidas de segurança para armazenamento seguro
(continua)

Ameaça	**Medida de segurança**
Tratamento ilegal dos dados	Controle de acessos
	Políticas de segurança
Divulgação indevida dos dados	Controle de acessos
	Políticas de segurança
Cópia ilegal	Controle de acessos
	Políticas de segurança
Engenharia Social	Políticas de segurança
	Treinamentos sobre segurança da informação
Modificação / alteração dos dados sem autorização	Controle de acessos
	Políticas de segurança
Ataques baseados em senhas	*Firewall*
	Sistema de detecção de invasão
	Antivírus / *anti-malware*
Acesso não autorizado	Firewall
	Controle de acessos
	Políticas de segurança
Acesso a links de fontes não conhecidas ou não confiáveis	*Firewall*
	Proxy systems

(conclusão)

Uso não autorizado de equipamentos	Controle de acessos
	Políticas de segurança
Software malicioso	Antivírus / *anti-malware*
	Controle de acessos

Fonte: Próprio autor.

3.3.4 Proteção à perda de dados

No capítulo da Lei 13.709 que trata de segurança da informação, um dos requisitos é a adoção de medidas técnicas para proteger os dados pessoais quanto a sua perda. Além da violação das regras impostas na legislação, a perda de dados pode oferecer grandes transtornos à organização, uma vez que estes dados podem ser relevantes para garantir a operação da mesma.

A perda de dados pode ocorrer por diversos motivos, como falhas em discos e dispositivos de armazenamento, furtos de equipamentos, códigos maliciosos que venham a comprometer os dados, incidentes naturais (alagamentos, vendavais, terremotos), incêndios ou por ação de indivíduos mal-intencionados. Apesar de medidas serem adotadas para manter os dados seguros (conforme apresentado na seção 3.3.3 deste trabalho), incidentes podem ocorrer, acarretando, por vezes, na destruição ou perda de informações da organização, incluindo dados pessoais. As medidas que devem ser adotadas, neste caso, são para garantir que os dados estejam disponíveis mesmo após a ocorrência de um incidente.

A Norma ABNT ISO/IEC 27002 (2005) dispões sobre a necessidade de se manter cópias de segurança para garantir a integridade e disponibilidade da informação na organização. Devem existir meios que garantam cópias das informações e dos recursos informáticos, como *softwares* para garantir que estes sejam recuperados após um desastre, em um tempo aceitável.

Alguns procedimentos devem ser adotados e precisam estar de acordo com as políticas definidas para geração das cópias de segurança. As cópias devem ser mantidas em local seguro, distante do local de origem, evitando que sejam vulneráveis aos mesmos desastres que possam ocorrer a este. A frequência da geração das cópias deve estar de acordo com as diretrizes propostas em políticas de segurança, e as mesmas devem ser testadas periodicamente, garantindo seu uso no caso de um incidente ocorrer. As mídias ou o local de armazenamento das cópias de segurança

deve respeitar as regras de controle de acesso, evitando que os dados sejam expostos a pessoal indevido.

Os dados pessoais devem ser incluídos nas informações salvas em cópias de segurança, garantindo que as mesmas não sejam perdidas caso ocorra um incidente que venha a causar sua indisponibilidade no local principal de armazenamento.

A implementação de um Plano de Continuidade de Negócios também deve ser considerada, com o objetivo de minimizar os impactos resultantes de um desastre e a recuperação das operações no menor tempo possível (SÊMOLA, 2003). O Plano de Continuidade de Negócios deve possuir as diretrizes e ações que devem ser tomadas na ocorrência de um desastre, apontando as responsabilidades de cada envolvido em retomar as operações da organização. A Norma ABNT ISO/IEC 27002 (2005) apresenta as diretrizes para implementação de um Plano de Continuidade de Negócios, apontando os aspectos que devem ser levados em conta neste processo. Os dados pessoais em poder da organização devem ser considerados como ativos críticos de informação na implementação do plano.

A implementação de um Plano de Continuidade de Negócios, aliado a geração e controle de cópias e segurança mantem os dados pessoais seguros quanto à sua perda por incidentes que possam ocorrer. O Quadro 9 apresenta as ameaças envolvidas e as medidas propostas.

Quadro 9 - Ameaças e medidas de segurança para proteção a perda de dados

Ameaça	**Medida de segurança**
Dano físico a mídia	Plano de Continuidade de Negócios
	Cópias de segurança
Comprometimento dos dados	Plano de Continuidade de Negócios
	Cópias de segurança
Furto de equipamentos	Plano de Continuidade de Negócios
	Cópias de segurança
Desastres físicos	Plano de Continuidade de Negócios
	Cópias de segurança

Fonte: Próprio autor.

3.3.5 Garantia da disponibilidade dos dados

A Lei 13.709 não requisita explicitamente que os dados estejam disponíveis em sua totalidade. Porém, convém que a organização mantenha seus sistemas de informação sempre aptos a responder às demandas, tanto dos objetivos da organização, quanto aos requisitos das normas e legislações vigentes. Segundo a Lei 13.709, os titulares podem solicitar informações sobre seus dados a qualquer momento, e essa informação deve estar disponível para ser entregue quando solicitada.

A garantia da disponibilidade de dados e informações se baseia na implantação de um Plano de Continuidade de Negócios, apresentada na seção 3.3.4 deste trabalho. As diretrizes de um plano de continuidade de negócios permitem que a organização não interrompa suas operações críticas no caso de um desastre ou incidente venha a acontecer. Quanto menor o tempo de resposta para um evento, menores os prejuízos para a empresa (KIM; SOLOMON, 2014).

A implementação de medidas depende dos objetivos adotados pela organização. Se a disponibilidade dos dados é crítica, devendo estar totalmente disponível, o tempo todo, as medidas a serem adotadas devem seguir diretrizes que garantam esta disponibilidade. Se a necessidade desta disponibilidade não é tão grande, as medidas adotadas podem ser de menor grandeza. A análise destas questões deve ser realizada ao se criar um Plano de Continuidade de Negócios.

Como forma de classificar o nível desejado para continuidade de negócios, podem ser adotadas medidas conforme descrito no Quadro 10 (SÊMOLA, 2003; KIM, SOLOMON, 2014). As medidas descritas são aconselháveis, não obrigatórias, pois a escolha das estratégias depende diretamente do nível de tolerância da organização quanto ao tempo de retorno das operações, do orçamento disponível para implementação das medidas propostas e do nível de risco que a empresa está disposta a correr. Maiores detalhes sobre medidas para continuidade de negócios estão disponíveis em literatura (SÊMOLA, 2003; KIM, SOLOMON, 2014; FONTES, 2006; ABNT, 2005).

Quadro 10 - Estratégias de centros de dados para recuperação de desastres

Estratégia	Descrição	Características
Hot-site	Estratégia que está pronta para entrar em operação assim que um incidente ocorrer.	Redundância de infraestrutura, canais de comunicação, de energia e armazenamento. Assim que houver falha no sistema original, uma "cópia" entra em operação no menor tempo possível. Pode ser citado como exemplo a implantação de um sistema espelhado de processamento de informações, em locais distintos. Quando um desses sistemas para de operar, por algum motivo, o outro entra em operação instantaneamente. Custo elevado de implementação.
Warm-site	Estratégia em que a organização tem uma tolerância maior de tempo de resposta a um incidente.	Utilização de medidas que mantenham a organização em operação após um incidente, mas que demanda mais tempo para voltar as operações após um incidente. Pode ser exemplificado como um sistema de e-mails, que perde sua conexão de comunicação. O retorno das operações leva alguns minutos, mas não causa impactos sensíveis as operações da organização. Outro exemplo pode ser a falta de energia, que pode ser suprida com a utilização de *no-breaks* até que o fornecimento seja reestabelecido, havendo o risco de que o tempo de retorno seja maior que a capacidade de trabalho do *no-break*.
Cold-site	Estratégia em que os recursos de infraestrutura são mínimos, existindo uma tolerância maior de resposta a incidentes.	Opção onde as medidas de recuperação demandam um maior tempo, provavelmente com substituição de equipamentos e carregamento de dados, *software* e *hardware* no novo local. Custo relativamente baixo de implementação, mas grande risco de indisponibilidade.

Fonte: Próprio autor.

A implantação de medidas para manter os dados disponíveis depende diretamente dos objetivos de uma organização, do tempo que a mesma pode ficar indisponível após um incidente ou desastre, e do orçamento disponível para implantar as medidas cabíveis. De qualquer forma, um Plano de Continuidade de Negócios, com estratégias bem definidas para contingência, deve ser implementado. Este plano deve conter as responsabilidades e as ações necessárias a cada um dos riscos que a empresa está vulnerável. As normas ABNT ISO/IEC 27002 (2005) e ABNT ISO/IEC 27005 (2008) apresentam as diretrizes para auxiliar na implementação de um Plano de Continuidade de Negócios.

3.3.6 Gerenciamento da segurança dos dados

O gerenciamento da segurança dos dados em uma organização parte da elaboração de um Sistema de Gestão da Segurança da Informação (SGSI). É um processo complexo, mas apresenta as diretrizes para controlar e manter todas as outras medidas de segurança necessárias à organização. O SGSI deve possuir uma Política de Segurança da Informação, a qual estabelece o grau de importância da informação para a empresa, a importância dos sistemas de informação os objetivos da organização em manter tal política (OLIVEIRA, 2001; ABNT, 2013). A Norma ABNT ISO/IEC 27001 (ABNT, 2013) apresenta as diretrizes para implementação de um SGSI em uma organização, independentemente do tipo ou tamanho. Para complementar, a Norma ABNT ISO/IEC 27002 (ABNT, 2013) demonstra as técnicas de segurança e os controles necessários para implementar um SGSI.

O SGSI deve ser implementado com conhecimento da organização. O conhecimento dos riscos que podem afetar a segurança da informação é fundamental para implementação de um sistema de segurança sólido. A Norma ABNT ISO/IEC 27005 (ABNT, 2008) apresenta as diretrizes para gestão dos riscos em uma organização.

Utilizando as três normas citadas anteriormente, uma organização consegue implementar um SGSI completo e abrangente, dentro de seus objetivos e que contemple todos os pontos necessários de controle.

Para atender os requisitos da Lei 13.709, um SGSI deve contemplar os controles apresentados nas seções anteriores deste capítulo, com as responsabilidades cabíveis a cada uma delas. Além disso, deve fornecer as diretrizes e as responsabilidades para fazer a comunicação da ocorrência de um incidente que envolva os dados pessoais em poder da empresa, de forma documentada e com a definição dos responsáveis para executar as ações necessárias.

As diretrizes para comunicar um incidente, conforme descrito na Lei, devem contemplar a maneira como a comunicação deve ser feita. Essa comunicação deve conter a ocorrência, quais os titulares de dados envolvidos, as medidas de controle de segurança que foram utilizadas para evitar que o incidente ocorresse, os riscos relacionados ao incidente, e as ações e métodos de contingência utilizados para

mitigar os efeitos do incidente. Deve estar explícita a forma como essa comunicação deve ser feita e quem são os responsáveis para executá-la.

Uma política de segurança da informação bem implementada deve ser conhecida por todos os colaboradores envolvidos, e todos devem saber suas responsabilidades quanto à segurança da informação e dos dados pessoais em poder da organização.

3.4 CONSIDERAÇÕES FINAIS

O atendimento à Lei 13.709, no que diz respeito a meios informáticos e técnicas de segurança da informação, se baseia fundamentalmente na implementação de um SGSI na organização. Conforme as diretrizes apontadas na norma ABNT ISO/IEC 27001 (ABNT, 2013), a organização deve conhecer seus objetivos, sua estrutura, os riscos a que está sujeita, para fazer um planejamento coerente das medidas de segurança que devem ser implementadas. Este planejamento deve contemplar os requisitos da Lei, com o objetivo de manter os dados pessoais em seu poder de forma segura, conforme estipulado pela mesma. É coerente que exista este planejamento prévio, documentado em políticas de segurança, e todos os envolvidos devem estar cientes de suas responsabilidades, para que as medidas de segurança adotadas pela empresa tenham o efeito esperado.

Com o conhecimento dos processos onde é necessário implementar e controlar medidas de segurança da informação, as ações a serem tomadas se tornam mais fáceis. Estas medidas não significam, unicamente, a proteção aos dados pessoais em poder da organização, mas representam a preservação de toda informação relevante aos negócios da mesma. Desta maneira, os dados pessoais devem ser tratados como uma informação confidencial da organização, como um ativo de grande importância para a mesma

As medidas técnicas de segurança apresentadas neste capítulo têm caráter bem abrangente. Desta forma, a definição de quais devem ser implementadas em uma organização deve se basear nos objetivos e requisitos das políticas de segurança. Como as organizações não são iguais umas às outras, não existe uma obrigatoriedade de adoção de todas as práticas apresentadas neste capítulo. Cada organização possui seus respectivos riscos de segurança, e a implementação de

medidas de segurança devem considerar tais riscos. Também deve ser observado o orçamento disponível pela organização para implementação de tais medidas. Uma empresa de pequeno porte provavelmente não adotará as mesmas medidas de uma empresa de grande porte.

Após apresentar as principais medidas que podem ser adotadas para manter os dados pessoais em segurança, conforme os requisitos estabelecidos na Lei 13.709, o próximo capítulo descreverá a proposta de solução deste trabalho.

4 PROPOSTA DE SOLUÇÃO

A proposta de solução para este trabalho consistiu na seleção de três empresas, a fim de analisar seu conhecimento da Lei 13.709 e realizar o levantamento do nível de segurança e das medidas de segurança da informação implantadas em relação à proteção de dados pessoais. Isso permitiu criar um panorama atual das organizações, a fim de definir as medidas técnicas de segurança da informação que deveriam ser implementadas para atender os requisitos da Lei e, por fim, criar uma proposta razoável a cada organização para implementação das ferramentas e medidas faltantes para o atendimento aos requisitos da Lei.

Para realização da proposta, foi definida a utilização do método de pesquisa exploratória com múltiplas fontes (estudos de caso), numa abordagem qualitativa. A pesquisa exploratória, segundo Creswell (2010), busca entender o significado que os indivíduos atribuem a um problema, analisando os dados coletados no ambiente da organização a partir das particularidades interpretadas para um contexto geral. Este método de pesquisa apresenta um resultado mais flexível, com foco na individualidade de cada organização estudada. Segundo Gil (2009), o estudo de caso exploratório busca uma visão mais acurada do problema para, posteriormente, construir uma hipótese capaz de orientar outras etapas do trabalho, ou trabalhos futuros.

A partir deste contexto, foi realizado o planejamento das atividades a serem desenvolvidas, as quais são:

1. Aplicação de questionário, buscando a compreensão cenário das organizações que estavam sendo estudadas neste trabalho, em relação a entendimento dos requisitos da Lei 13.709 e as medidas de segurança da informação implantadas;
2. Análise do cenário de cada organização, no que diz respeito aos aspectos de segurança atuais e os objetivos quanto a proteção de dados pessoais;
3. Elaboração de um panorama geral sobre a visão das organizações em relação a Lei 13.709 e suas responsabilidades;

4. Levantamento das necessidades individuais de cada organização quanto a implementação de medidas e ferramentas de segurança da informação para o atendimento à Lei 13.709;
5. Elaboração e apresentação de propostas de melhorias para cada organização, com o objetivo do atendimento total da Lei 13.709;
6. Aplicação do questionário final, com objetivo de analisar a aceitação das propostas apresentadas;
7. Avaliação dos resultados.

4.1 SELEÇÃO DAS ORGANIZAÇÕES

A seleção das empresas onde os estudos de caso foram realizados foi baseada nos seguintes critérios:

a) A organização deve possuir dados pessoais em seu poder, armazenados de forma digital;
b) A organização deve contar com setor de Tecnologia da Informação implementado;
c) A organização deve dispor de facilidade de acesso a diretores, gestores e responsáveis pela área de Tecnologia da Informação, a fim de responder aos questionários e entrevistas propostos.

Nas subseções seguintes, são apresentados os casos selecionados para realização dos estudos de caso. Como forma de manter a confidencialidade, os nomes das empresas não são revelados, bem como obteve-se o cuidado de não informar dados que pudessem expor tanto a empresa quanto funcionários ou pessoas ligadas a mesma.

4.1.1 Caso 1 – Empresa Alfa

A empresa Alfa é um órgão público, instituído na cidade de Caxias do Sul desde maio de 2004. Atua com o atendimento direto ao público, recebendo e gerando informações diariamente sobre reclamações, consultas e denúncias de cidadãos.

Apesar de ser um braço de uma entidade a nível nacional, a área de abrangência de suas operações é regional, aplicada somente à cidade de Caxias do Sul.

Sua organização interna compreende áreas de atendimento direto ao público, área jurídica, secretarias e fiscalização. Além destas áreas, existem diferentes programas executados na comunidade da cidade de Caxias do Sul, onde todos envolvem a coleta e tratamento de dados pessoais.

Desde o ano de 2007, tem capacidade de atendimento de cerca de 200 pessoas por dia, gerando uma grande quantidade de dados pessoais em seu poder. Além do atendimento direto, em sua sede, é possível preencher formulários em seu site, onde dados pessoais podem ser enviados e armazenados pela empresa. Também possui tratamento jurídico de informações, onde podem existir dados sensíveis, de indivíduos ou empresas, armazenados em seus bancos de dados. Além de serviços que se aplicam a tratamento de dados pessoais com fins diretamente ligados aos titulares, a empresa oferece dados de pesquisa, utilizando os dados fornecidos pelos indivíduos e por outras organizações.

Em resumo, a empresa Alfa realiza coleta e tratamento de dados pessoais de seus funcionários, do público ao qual atende e, também, para fins de pesquisa, dados pessoais que podem ser recebidos de outras organizações.

4.1.2 Caso 2 – Empresa Beta

A empresa Beta atua no ramo de agronegócios e desenvolvimento de tecnologias genéticas para cultivo de hortaliças. Possui sede na serra gaúcha, atuando há aproximadamente 40 anos neste ramo.

Os produtos da empresa são distribuídos para todo o Brasil. Também possui laboratório para desenvolvimento de novas tecnologias e testes em seus produtos. A distribuição é feita através de representantes cadastrados na empresa. Além dos distribuidores, existe um canal de venda *on-line*, onde os clientes podem se cadastrar e realizar a compra dos produtos diretamente pela *internet*. O desenvolvimento das tecnologias de TI é feito internamente, portanto, existe uma área bem estruturada no que diz respeito a sistemas de informação.

De forma geral, a empresa possui dados pessoais de seus funcionários e colaboradores, de fornecedores, dos clientes que realizam cadastro em seu *e-commerce*, além dos clientes tratados pelos representantes da empresa.

4.1.3 Caso 3 – Empresa Gama

Empresa do ramo moveleiro situada em Caxias do Sul, a Gama atua no mercado desde a década de 1940, porém, somente em 1985 atua na produção de móveis com projeto e designs autorais.

Em sua sede, realiza a fabricação dos móveis, os quais são vendidos ao cliente final através de lojas autorizadas. A venda direta ocorre somente a clientes corporativos, como hotéis, pousadas ou *resorts*. Os produtos da empresa Gama são comercializados em todo o Brasil, e em alguns países no exterior.

A empresa possui um setor de TI estruturado em sua sede, o que auxilia na realização da proposta deste trabalho. Os dados pessoais que estão em seu poder são: dados de funcionários e colaboradores, dados de clientes, dados de lojistas e dados de fornecedores.

4.2 QUESTIONÁRIO DE PESQUISA SOBRE REQUISITOS DA LEI 13.709 E ATUAL CENÁRIO DAS ORGANIZAÇÕES

A primeira etapa realizada foi a aplicação de um questionário com perguntas fechadas, o qual teve por objetivo verificar a percepção e entendimento das organizações quanto as suas responsabilidades no atendimento aos requisitos da Lei 13.709, como também analisar como as empresas tratavam a segurança da informação e de dados pessoais. Foram avaliados o entendimento e a preocupação quanto à segurança da informação, o conhecimento dos riscos e das ameaças, e quais medidas e ferramentas já estavam implementadas em cada organização.

O questionário aplicado procurava, como objetivo primário, perceber o nível de entendimento dos envolvidos e da empresa quanto aos requisitos da Lei 13.709 e analisar a situação da organização quanto à preocupação sobre a segurança da informação. Como objetivos secundários, identificar qual a percepção da empresa quanto ao impacto que a aprovação da Lei teria sobre a mesma e o conhecimento sobre a maneira que os dados pessoais eram tratados pelos envolvidos, como

também analisar qual a percepção da organização quanto às ameaças presentes na organização e quais as ferramentas já eram utilizadas para minimizar tais riscos. O questionário está disponível no Apêndice A deste trabalho.

O questionário é dividido em seções, onde a primeira apresenta questões referentes à percepção da Lei 13.709, a segunda seção se refere aos dados pessoais em poder da empresa, a terceira parte aborda a gestão da segurança e a quarta apresenta questões referentes a medidas de segurança implementadas. As perguntas serão fechadas, ou seja, terão alternativas definidas para cada questão como respostas. A utilização deste método de questionário permite uma análise qualitativa posteriormente. Para planejamento e análise da elaboração do questionário, foram utilizados métodos descritos na literatura (YIN, 2015; GIL, 2009; VIEIRA, 2009; GIL, 2008).

O público alvo definido para responder os questionários foram os gestores das organizações e os responsáveis pela infraestrutura e sistemas de informação destas. Foram selecionados os gestores da organização, com a finalidade de verificar a preocupação que os mesmos possuem quanto à segurança da informação e dos dados pessoais em poder da organização e os responsáveis pela área de TI para obter informações pertinentes aos sistemas de informação e de segurança da informação da empresa.

Terminada a coleta de dados, foi desenvolvido um panorama das organizações através da análise dos resultados da pesquisa realizada, a fim de desenvolver a proposta de solução deste trabalho.

4.3 ANÁLISE DAS RESPOSTAS DO QUESTIONÁRIO

Após a aplicação do questionário definido na seção anterior, foram avaliadas as respostas obtidas e realizada uma análise para buscar compreender quais dados pessoais a empresa possuía em seu poder, quais as medidas já adotadas para manter em segurança estes dados e identificar as ameaças que poderiam afetar os mesmos. A análise das respostas foi complementada com visitas às organizações, as quais são abordadas na Seção 4.4.

A análise verificou, primeiramente, as respostas obtidas quanto ao entendimento da Lei 13.709 por parte das empresas, procurando perceber como a

empresa estava abordando a aprovação da Lei e se já existia algum projeto em andamento para se adequar aos requisitos impostos pela mesma. Foi analisado, posteriormente, como a empresa tratava os dados pessoais em seu poder, verificando quais tipos de dados a mesma possuía e como esses dados eram armazenados e manipulados. Também foram verificadas quais as medidas de segurança da informação já eram implementadas em cada organização, confrontando as respostas do questionário com as ferramentas e medidas pesquisadas na literatura e apresentadas no Capítulo 3.

A fim de atender os objetivos anteriormente descritos, a análise do questionário levou em consideração os seguintes pontos:

a) o conhecimento sobre os aspectos da Lei 13.709 deve ser de conhecimento da área de TI e dos gestores das organizações;

b) a compreensão do que são dados pessoais e de quais dados pessoais a empresa possui poder deve ser pertinente tanto à área de TI quanto aos gestores da organização;

c) o conhecimento sobre políticas de segurança e sobre a possível implantação de um SGSI deve ser de conhecimento tanto da área de TI quanto dos gestores da organização;

d) o conhecimento sobre ferramentas e medidas de segurança implantados é responsabilidade da área de TI das organizações;

e) o conhecimento sobre ameaças e riscos que cercam a informação nas organizações é, também, relacionado à área de TI.

Como resultado desta análise, era esperado que, por possuírem dados pessoais em seu poder, as empresas selecionadas possuíssem conhecimento da necessidade de manter esses dados de forma segura, tanto na área de TI, quanto nas áreas gerenciais das mesmas. Em relação à segurança da informação, esperava-se que as organizações já possuíssem ferramentas e medidas implementadas. Era esperado que essas medidas provavelmente focassem a segurança de informações pertinentes aos negócios da empresa, não se estendendo aos dados pessoais da forma que a Lei 13.709 propõe.

4.4 ELABORAÇÃO DO PANORAMA GERAL SOBRE A VISÃO DAS ORGANIZAÇÕES

Após a análise individual de cada organização quanto ao conhecimento dos requisitos da Lei 13.709 e as medidas de segurança da informação já implementadas em cada organização, foi elaborado um panorama geral sobre a visão das empresas selecionadas quanto ao tema abordado neste trabalho.

Para auxiliar na elaboração deste panorama, foram realizadas visitas às organizações selecionadas, a fim de visualizar os processos realizados nas mesmas e ter uma melhor compreensão das operações que incluíam a manipulação de dados pessoais. A observação e compreensão dos processos e de como a empresa estava estruturada foi essencial para complementar a análise dos dados extraídos no questionário aplicado, ajudando a entender onde existia a necessidade de aplicação, tanto das normas da Lei, quanto as medidas de segurança da informação.

O panorama foi elaborado com fim informativo, apresentando qual o conhecimento e comprometimento com a Lei 13.709 de forma geral, e agrupando as análises das pesquisas realizadas nas organizações. Assim, pôde-se ter uma visão da receptividade da aprovação da Lei por parte das organizações, de uma forma mais generalizada. Como hipótese, era possível que as organizações não tivessem o preparo necessário para atender os requisitos propostos na Lei, ou, até mesmo, o conhecimento de todo o regramento imposto pela mesma.

Também se tornou possível visualizar como é o gerenciamento e implementação de ferramentas e medidas de segurança da informação de forma geral, agrupando os resultados dos questionários aplicados. As empresas selecionadas, pelo porte que possuem, provavelmente já possuíssem, implementadas, ferramentas que garantiriam a segurança das informações internas, pertinentes ao negócio das mesmas. Porém, de forma geral, os dados pessoais poderiam não estar incluídos neste nível de proteção.

A elaboração deste panorama serviu, principalmente, para demonstrar como a aprovação da Lei 13.709 está sendo observada pelas organizações e como estas estavam se preparando para implementar os requisitos impostos.

4.5 LEVANTAMENTO DAS NECESSIDADES INDIVIDUAIS DE CADA ORGANIZAÇÃO

Esta etapa do trabalho consistiu de um estudo das medidas e ferramentas de segurança da informação que precisariam ser implementadas para cada organização, a fim de cumprir plenamente os requisitos impostos pela Lei 13.709.

Analisando as respostas dos questionários aplicados nos estudos de caso, juntamente com as visitas realizadas, foi possível perceber se havia a compreensão dos requisitos impostos pela Lei 13.709. Também foi possível avaliar os dados pessoais que a empresa possuía, sua preocupação em manter estes dados em segurança e a situação de cada empresa no que diz respeito a ferramentas e medidas de segurança da informação implementadas. Assim, foi possível fazer uma relação com as necessidades impostas pela Lei.

No contexto apresentado, para cada uma das ferramentas e medidas apresentadas para transmissão segura de dados, controle de acessos, proteção contra vazamento de dados, proteção à integridade dos dados, proteção quanto à perda indevida dos dados, garantia de disponibilidade dos dados e gerenciamento da segurança dos dados, deveria ser observado se a empresa possuía os cuidados necessários implantados, como estavam implantados e se realmente satisfaziam as normas estabelecidas na Lei 13.709. Cabe observar que, dependendo dos processos e das necessidades individuais de cada organização, talvez nem todas as ferramentas deveriam ser implementadas. Também seria possível que alguma medida ou ferramenta pudesse estar implementada de forma incompleta ou que não satisfizesse o nível de segurança desejado para atender os requisitos da Lei.

No caso de alguma medida ou ferramenta não estar implementada de maneira satisfatória conforme as necessidades impostas pela Lei, a mesma foi sugerida como melhoria para cada uma das organizações

4.6 ELABORAÇÃO E APRESENTAÇÃO DAS PROPOSTAS DE MELHORIA PARA AS ORGANIZAÇÕES

Com base nas análises feitas para cada organização, foi elaborado um documento direcionado a cada uma das empresas, apresentando sugestões de

implementação ou melhoria de ferramentas e medidas de segurança da informação, com o objetivo de atender os requisitos da Lei 13.709.

O documento foi direcionado aos gestores da organização e gestores da área de TI. Neste documento, foram descritas as necessidades de melhoria observadas nas análises anteriormente definidas, juntamente com a justificativa da implementação de cada uma delas.

4.7 AVALIAÇÃO FINAL DA APLICAÇÃO DOS ESTUDOS DE CASO

Após a apreciação do relatório elaborado para cada um dos estudos de caso, uma avaliação foi realizada, com o intuito de verificar a percepção e aceitação de cada organização quanto as alterações e implementações propostas para o atendimento da Lei 13.709.

Foi utilizado o método de entrevista como forma de evidenciar a aceitação das propostas. A entrevista, segundo Gil (2009), é uma técnica que permite a obtenção de dados em profundidade nos mais diferentes aspectos. Além disso, é uma técnica que permite flexibilidade e adaptação conforme a entrevista é conduzida. A entrevista foi do tipo guiada, onde as perguntas são pré-determinadas, mas a ordem e a formulação das mesmas durante a entrevista poderiam ser alteradas, dando flexibilidade para adequar o curso da mesma conforme características do entrevistado.

As entrevistas foram direcionadas aos gestores da área de TI das organizações e aos gestores das organizações. A preparação para as mesmas ocorreu na seguinte ordem:

1. Elaboração do questionário guia, disponível no Apêndice B;
2. Agendamento das entrevistas;
3. Realização da entrevista;
4. Análise e elaboração de uma conclusão.

A análise dos resultados foi elaborada pela técnica clássica apontada por Gil (2009). Esse método procura reunir, organizar e sumarizar os dados de forma a explorar de forma mais aprofundada um determinado assunto. Esperava-se, com isso, montar uma visão de como foi a receptividade das organizações quanto às melhorias

que deveriam ser realizadas com a aprovação da Lei 13.709 e como as mesmas providenciariam as adequações necessárias para atender os requisitos da Lei.

5 ESTUDOS DE CASO

Conforme proposto no Capítulo 4, a primeira etapa para análise dos casos selecionados foi a aplicação do questionário apresentado no Apêndice A. Juntamente ao questionário, visitas foram realizadas nas empresas, a fim de evidenciar fatos que poderiam não estar claros somente com a análise das respostas recebidas. Durante as visitas, também se pôde perceber como são realizados os processos de tratamento dos dados.

Com os retornos dos questionários aplicados e demais informações, foi possível realizar a análise qualitativa de cada caso. A análise contempla, primeiramente, a apresentação do panorama atual de cada organização em relação a segurança da informação e conhecimento geral da aprovação da Lei 13.709/18. Tal panorama procura evidenciar somente o posicionamento de cada um dos casos estudados.

Posteriormente, para cada um dos casos, foi realizada uma análise qualitativa, com o objetivo de verificar se os controles e medidas adotados pelas empresas para manter a segurança dos dados estão de acordo com as práticas estudadas na literatura e apresentadas no Capítulo 4, em acordo com os requisitos impostos pela Lei 13.709/18.

Com base na análise de cada caso, foi possível elaborar as propostas de melhoria, as quais foram apresentadas para cada uma das empresas estudadas, a fim de se obter um retorno sobre sua validade e possível implementação futura. A seguir são apresentados os resultados e propostas de melhoria para cada um dos casos selecionados para realização desse trabalho.

5.1 CASO 1 – EMPRESA ALFA

A Empresa Alfa, conforme observado na Seção 4.1 desse trabalho, é uma empresa de direito público, de atendimento direto ao público em geral. Para coleta de informações e dados, além da pesquisa, foi realizada uma visita ao local, onde pôde-se ter uma visão melhor dos processos realizados.

5.1.1 Panorama atual – Empresa Alfa

A primeira etapa da análise realizada para o Caso 1 constitui da elaboração de um panorama atual de como a empresa trata tanto a aprovação da Lei, quanto a segurança da informação e dos dados em seu poder.

A Empresa Alfa buscou conhecer os requisitos impostos pela Lei 13.709/18, principalmente no âmbito jurídico e burocrático. Conforme retorno do questionário e observações feitas na visita realizada, a empresa levou o assunto para reuniões gerenciais, buscando apoio da direção para realizar as mudanças necessárias para atender os requisitos impostos pela Lei. Além de buscar entender os requisitos da Lei, a empresa também procurou alternativas para atendê-los e possui projetos em andamento para tal.

O armazenamento de dados pessoais da Empresa Alfa é feito em bancos de dados dedicados, tanto de fornecedores, clientes e funcionários. Ao realizar atendimento ao público, os dados são preenchidos em formulários físicos que, posteriormente, são cadastrados em um sistema com base nacional.

A empresa também utiliza dados pessoais para realização de pesquisas e dados estatísticos. Esses dados, segundo constatado, podem ser relacionados com seus titulares, não atendendo os requisitos impostos pela Lei. Também existe a possibilidade de acessar as informações prestadas pelo público, de maneira física, assinando termos de compromisso internos da instituição. Questionados sobre a prática, a empresa informou que, por se tratar de processos públicos, é permitido que se realize tal consulta, de forma legal, desde que exista o termo de compromisso assinado.

A empresa informou que possui uma Política de Segurança da Informação documentada e divulgada para os colaboradores, a qual é revisada periodicamente, incluindo, também, os riscos iminentes a segurança da informação, a fim de melhorar as práticas para proteção de dados na empresa. A política da segurança conta, também, com o apoio e comprometimento da direção da organização.

A empresa informou, também, que possui políticas documentadas para controle de acessos na empresa, a qual é divulgada para todos os colaboradores, para que estes conheçam suas responsabilidades e deveres em relação à utilização de

sistemas de informação na organização. Também existe controle no acesso de clientes, visitantes e fornecedores dentro das dependências da empresa, os quais não podem circular desacompanhados e não possuem acesso a rede de dados da mesma. Para complementar, existem registros de atividades efetuadas na rede da empresa.

Para minimizar os riscos quanto ao armazenamento seguro dos dados, a empresa Alfa adota medidas como restrições de uso de dispositivos pessoais, como *smartphones*, *tablets* ou *notebooks,* diferentes privilégios de acesso a arquivos e dados na rede, limitação das atividades dos funcionários em seus computadores, não sendo permitido instalar *softwares* ou alterar configurações.

Os sistemas e computadores são regularmente auditados a fim de verificar se existem softwares não autorizados instalados, bem como existem programas antivírus atualizados instalados nessas máquinas. Não existe possibilidade de trabalho remoto na empresa.

Na visita realizada, pôde-se constatar que a administração dos sistemas é realizada pela Prefeitura de Caxias do Sul, sem o envolvimento do pessoal da Empresa Alfa. Dessa maneira, não foi possível verificar se existem sistemas de *firewall, proxy* ou detecção de invasão de rede implantados. Também não foi possível identificar como são tomadas medidas quanto a perda indevida de dados, nem sobre transmissão segura de dados e continuidade de negócios.

5.1.2 Análise do panorama atual – Empresa Alfa

A Empresa Alfa, como se pôde verificar, utiliza dados pessoais em todos os processos de trabalho executados na organização. Os processos incluem a coleta de dados, de forma física em formulários e relatórios e a inclusão destes dados em sistema informatizado, desenvolvido para os serviços prestados pela mesma.

Por se tratar de uma empresa pública, todo o serviço de manutenção e controle de infraestrutura de TI é prestado pela Prefeitura de Caxias do Sul. Contudo, é aconselhável adotar práticas de segurança da informação para proteger os dados, tanto da organização quanto pessoais, protegidos de ameaças que podem comprometer os mesmos.

Primeiramente, é aconselhável que se tenha uma política de segurança da informação implementada, com o apoio da direção tanto para sua devida manutenção e divulgação aos funcionários e envolvidos. A política de segurança da informação deve possuir, claramente, os objetivos da organização e todas as definições quanto a objetivos e princípios para orientar as atividades de segurança da informação, além de atribuir as responsabilidades aos envolvidos. O escopo da política de segurança deve estabelecer, também, os limites até onde é possível se ter controle da informação em poder da organização, levando em conta que os serviços de TI são providos pela Prefeitura de Caxias do Sul.

Uma política de análise de riscos deve ser implementada, avaliando os ativos de informação em poder da empresa (principalmente os ativos tratados de forma física), as ameaças que podem atingir esses ativos, as vulnerabilidades que podem permitir que as ameaças atinjam os ativos e os controles já utilizados para manter a segurança destes. Isso torna possível definir os riscos envolvidos na segurança da informação e como tratar estes. A política deve prover os métodos de análise, as responsabilidades e os meios de análise crítica de forma cíclica, mantendo os processos atualizados e a melhoria contínua da análise.

Com base nos riscos avaliados, outros procedimentos e políticas devem ser implementados, os quais envolvem:

a) política de controle de acesso;

b) política de segurança física do ambiente;

c) política de proteção e privacidade da informação de identificação pessoal;

d) política de contratações de serviços.

A política de controle de acesso deve prover os limites de acesso a informação, seja por meio lógico ou físico. Deve identificar os usuários ou grupos de usuários, definidos por suas funções dentro da organização, e quais as informações e dados que estes podem acessar. A política deve ser regularmente analisada, a fim de estar atualizada com os requisitos de negócio da empresa, requisitos legais e os riscos envolvidos no processo, bem como apresentar os responsáveis pela manutenção da política. Ao se definir os acessos, a empresa deve considerar os dados físicos presentes no ambiente de trabalho. Convém delimitar áreas que sejam consideradas

críticas, onde existem dados sensíveis ou informações restritas, o que será tratado adiante nesse trabalho. A política de controle de acesso deve identificar os ativos de informação, onde estes estão disponíveis, quem pode ter acesso a esses ativos e a maneira que o acesso é liberado. A adoção de termos de responsabilidade por propriedade dos ativos de informação e por acesso a esses é importante, considerando os meios de tratar situações de acesso indevido ou vazamento de informação.

O acesso por meio lógico também deve ser tratado, identificando os métodos de acesso a sistemas utilizados na empresa, por quem podem ser acessados e os privilégios de acesso a informação concedidos aos usuários. Apesar dos serviços de TI serem prestados por entidade externa a empresa, deve existir um regramento conforme os objetivos da organização, os quais devem ser informados e requeridos a empresa que presta os serviços de infraestrutura. Esse regramento deve ser de conhecimento geral dentro da organização, estipulando quem é responsável pela propriedade de cada grupo de informação ou dados, pela concessão de acesso e pela revisão dos privilégios concedidos.

Convém que a política de controle de acesso observe as maneiras de se excluir os acessos quanto estes não sejam mais utilizados ou necessários, como realocações de funcionários, desligamentos e mudanças estratégicas nas funções de funcionários.

Uma política de segurança física do ambiente deve ser implementada, a fim de estabelecer limites físicos a informação, prevenindo acesso não autorizado, danos e interferência nas informações tratadas na organização. Devem ser identificados os perímetros considerados críticos, onde dados e informações sensíveis são tratados ou armazenados, tanto de forma lógica quanto física. Essas áreas devem ser acessadas somente por pessoal autorizado, e esse acesso deve ser controlado ou registrado de alguma maneira. As áreas consideradas de segurança devem ser de conhecimento de todos os funcionários da empresa, que devem saber quais áreas podem ou não acessar. Convém que exista mais de um meio de controlar o acesso a essas áreas, o que pode ser auxiliado com câmeras de segurança, salas com fechaduras inteligentes, utilização de cofres ou armários trancados para armazenar documentos.

Como existe circulação de pessoas não ligadas ao negócio constantemente dentro da organização, convém que as áreas de segurança sejam definidas de forma a estarem protegidas do acesso ao público em geral. Salas de atendimento, recepção e salas de espera não devem conter informações consideradas sensíveis aos negócios ou que venham a expor dados de pessoas de forma indevida.

Deve existir a preocupação constante em relação a dados pessoais que estão presentes na organização. Convém que uma política para proteção e privacidade da informação pessoal seja implementada, estando em conformidade com a legislação vigente, principalmente a Lei 13.709. Esta deve conter informações sobre o que são dados pessoais, como preservá-los de acesso e tratamento indevido, as responsabilidades cabíveis aos funcionários da empresa e possíveis penalidades consideradas pela organização e pela legislação.

Como o serviço de manutenção de infraestrutura é realizado pela Prefeitura de Caxias do Sul, convém que seja implementada uma política de relacionamento de contratação de serviços, indicando os tipos de fornecedores, os serviços que estes prestam e quais informações podem ser acessadas por estes. Devem existir meios de controlar quais os acessos realizados pelos fornecedores de serviço, de responsabilizar os fornecedores por esses acessos e as obrigações destes para proteger os dados e informações da organização. Os envolvidos nos processos de contratação e acompanhamento de serviços realizados na organização devem estar treinados para oferecer somente o acesso necessário a informação e dados presentes na organização, conforme o serviço que necessita ser prestado.

Por fim, políticas orientadas aos usuários devem ser implementadas, indicando as melhores práticas de utilização de ativos de TI na empresa, a importância de manter documentos, papéis, mídias e similares protegidos de maneira a não serem acessados ou visualizados por pessoas não autorizadas. Políticas de mesa e tela limpa devem ser adotadas, procurando manter as informações sensíveis ou críticas seguras, sejam estas de forma lógica ou física, estando armazenadas em local seguro quando não estiverem em uso. Os funcionários também devem estar orientados sobrem formas seguras de transmissão de dados, quando necessário, bem como sobre utilização de equipamentos e dispositivos móveis dentro da organização, procurando manter a confidencialidade e segurança dos dados sensíveis a organização ou dados pessoais.

5.1.3 Análise final – Empresa Alfa

A empresa Alfa, após a apreciação da proposta de melhoria apresentada no Apêndice C, foi abordada com o objetivo de identificar sua perceptividade quanto ao conteúdo da mesma.

Durante entrevista realizada com o Coordenador Geral da mesma, pôde-se verificar que existe uma preocupação constante em buscar alternativas para manter seguros os dados pessoais presentes nas operações da empresa. Essa preocupação se estende por todo o conteúdo da Lei 13.709/18, não se baseando unicamente nos requisitos técnicos informáticos, assunto base desse trabalho.

As propostas apresentadas foram avaliadas como válidas e serão melhores estudadas quanto a sua futura implementação. Como o conteúdo da proposta apresentado buscou se limitar aos processos que são realizados e gerenciados pela empresa, excluindo processos que tratam do gerenciamento da infraestrutura de TI, os mesmos podem ser implementados pelo pessoal da própria organização.

Porém, existe o interesse, por parte da organização, em estender os estudos de melhorias que atendam aos requisitos da Lei para os serviços e intervenções realizados pela Prefeitura de Caxias do Sul, demonstrando interesse e preocupação em manter os dados pessoais em seu poder de forma segura com a adoção de medidas eficazes e que atendam as práticas apresentadas, principalmente, nas normas ABNT ISO/IEC da série 27.000.

Por fim, a empresa demonstrou interesse em trabalhos futuros, os quais possam vir a auxiliá-la em implementar e manter processos e práticas eficazes no que diz respeito a segurança da informação de forma geral e proteção de dados pessoais que estão em seu poder, como também demonstrou a intenção em apoiar possíveis trabalhos que possam ser desenvolvidos juntamente com a área de TI da Prefeitura de Caxias do Sul.

5.2 CASO 2 – EMPRESA BETA

A Empresa Beta é uma empresa de direito privado que atua com desenvolvimento genético para o ramo do agronegócio. Para verificar qual a atual situação quanto a segurança da informação e conhecimento da Lei 13.709/18, foi

aplicado o questionário de pesquisa apresentado no Apêndice A, complementado com uma visita realizada na empresa.

5.2.1 Panorama atual – Empresa Beta

A empresa Beta possui conhecimento da aprovação da Lei 13.709/18, porém, ainda não buscou maiores conhecimentos sobre seus requisitos e sobre quais medidas devem ser adotadas para atendê-los, como também não possui nenhum projeto em andamento para tal. Durante a visita, foi possível perceber que existe interesse nesse entendimento, tanto técnico quanto jurídico.

Os dados pessoais de funcionários, clientes e fornecedores são todos armazenados em bancos dedicados, situados na própria empresa. Alguns desses dados são utilizados para fins estatísticos e de pesquisa, porém, ainda podem ser relacionados com seus titulares quando assim utilizados. Além disso, a empresa realiza coleta de dados pessoais pela internet, através do canal de vendas na internet (*e-commerce*), como nome, CPF e endereço, além de dados financeiros (número de cartão de crédito ou conta bancária).

Não existe uma política de segurança da informação documentada na empresa Beta. A empresa busca conhecer os riscos, com a finalidade de melhorar as medidas de segurança adotadas, mas não existe um procedimento formal para isso. Durante a visita foi percebido que, apesar de não existir documentação, a empresa define os riscos conforme histórico informal de eventos que atingem a empresa, demonstrando baixa maturidade no processo. A adoção de controles de segurança se baseia também na experiência que outras empresas de mesmo porte adotam atualmente.

A empresa informou que realiza o controle de acessos a sistemas de informação, porém, não existe documentação. Os procedimentos adotados, segundo a empresa Beta, incluem: controle de acessos em sistemas de software, controle de circulação de pessoas que não pertencem ao quadro de colaboradores da empresa, perímetros de segurança definidos para a área de TI, senhas e privilégios de acesso revisados (não foi possível identificar a periodicidade) e impedimento de acesso à rede da empresa por fornecedores ou terceiros.

Para garantir que os dados não sejam acessados de forma indevida, a empresa adota medidas de restrição de acesso de várias maneiras. Os equipamentos de

armazenamento e servidores instalados na empresa são configurados para evitar acessos indevidos por agentes externos à rede, bem como evitando que dados saiam do ambiente interno de forma indevida (*firewall, proxy* e IDS). Os funcionários não podem utilizar mídias de armazenamento nos computadores da empresa, e a utilização de equipamentos pessoais somente é permitida com autorização de superiores e avaliação da área de TI. Os privilégios de acesso a informação da empresa também são controlados, evitando que se tenha acesso a dados não relevantes para as atividades de cada funcionário, mas essa prática não conta com um procedimento que evidencie as regras adotadas.

A empresa adota medidas para evitar perda indevida de dados, realizando backups dos sistemas, bem como testes de mídia e recuperação eventualmente, mas o processo não conta com uma política ou regramento documentado dos procedimentos.

A utilização de pontos remotos de trabalho com criptografia, utilização de VPN, proteção de e-mail (criptografia e PGP) e protocolos de comunicação atuais, como IPv6, auxiliam para que a transmissão de dados seja executada com segurança.

Apesar de não existir um plano de continuidade documentado, a empresa adota medidas para manter os serviços operantes, no caso da ocorrência de um incidente. Existem redundâncias de sistemas e servidores, além de links de internet e de energia, para que os serviços não fiquem indisponíveis por muito tempo se ocorrer um incidente.

5.2.2 Análise do panorama atual – Empresa Beta

A Empresa Beta mostrou conhecer a aprovação da Lei 13.709/18. Contudo, ainda é necessário que a mesma obtenha maiores detalhes sobre os requisitos impostos, se adequando não somente de forma técnica, como também de forma jurídica. Esse assunto deve, portanto, ser tratado em reuniões gerenciais de forma estratégica, avaliando a adoção de projetos de adequação de processos e adequações técnicas, que serão apresentadas no decorrer dessa seção. Não somente a área de TI deve ser envolvida nesse processo de entendimento da Lei, mas todas as áreas que tem contato com dados pessoais (de forma física ou lógica).

Como pôde ser verificado, a empresa não possui uma política de segurança implementada. Para garantir que todos os outros processos de controle de segurança sejam eficazes, a Norma ABNT ISO/IEC 27002 (ABNT, 2013) orienta que deve existir um conjunto de políticas de segurança da informação, aprovado pela direção, publicado e comunicado a todos os funcionários e partes externas relevantes. Essa diretriz deve partir da alta direção, a qual deve dar apoio e solicitar a todos os envolvidos que pratiquem a segurança da informação conforme estabelecido nas políticas e procedimentos adotados na organização.

A política de segurança da informação deve conter requisitos oriundos de estratégias do negócio, regulamentações, legislação (incluindo a Lei 13.709). Também deve possui definições quanto a objetivos e princípios que orientem as atividades relativas à segurança da informação, atribuição de responsabilidades para o gerenciamento da segurança da informação e os processos utilizados para o tratamento de desvios e exceções. As políticas devem ser analisadas a intervalos pré-definidos, ou quando mudanças significativas ocorrerem, assegurando que a mesma esteja atualizada e adequada as necessidades da organização.

É importante ter uma política de segurança da informação para prover os recursos necessários, oriundos da direção, em apoio à abordagem do gerenciamento dos objetivos da segurança da informação. Para auxiliar essa diretriz principal, devem existir normas e políticas de dimensão, específicas para grupos de controles de segurança, as quais abrangem tanto os sistemas lógicos de informação, como informações em forma física (relatórios, documentos impressos e similares).

Para controles de acesso, a empresa deve criar uma política específica, com o objetivo de limitar o acesso à informação e aos recursos de processamento da informação. A empresa conta com controles implementados atualmente, mas que, isoladamente e sem um procedimento que padronize seu uso, pode representar falhas e proporcionar brechas para que informações sejam visualizadas ou acessadas por pessoas não autorizadas ou de forma indevida.

Devem ser considerados, para elaborar a política de controle de acesso, o acesso lógico e físico aos dados e a informação. Conforme aconselhado pela Norma ABNT ISO/IEC 27002 (ABNT, 2013), o regramento da política de controle de acesso deve conter itens conforme representado no Quadro 11.

Quadro 11 - Regras para política de acesso

(continua)

Controle	Descrição
Acesso à rede e serviços de rede	Deve ser definido os serviços de rede que são permitidos de acesso, bem como o procedimento adotado para determinar as permissões de acesso. Definição dos meios utilizados para acessar redes externamente (VPN ou acesso remoto). Definição dos métodos de autenticação utilizados. Procedimentos e controles de gerenciamento para proteger o acesso a conexões de rede (*firewall* ou IDS). Formas de monitoramento do uso das conexões de rede.
Gerenciamento do acesso do usuário	Diretrizes documentadas do registro e cancelamento do acesso do usuário a redes de dados e sistemas da empresa. Procedimento documentado para imediata exclusão dos acessos quando o usuário não mais precisar. Métodos para monitorar regularmente os acessos concedidos. Registro do conhecimento do usuário sobre seus direitos e responsabilidades quanto ao acesso aos dados, bem como de sua ciência sobre a importância em manter sigilo sobre credenciais e senhas em seu poder.
Gerenciamento dos privilégios de acesso	Controle sobre o que cada usuário pode ou não acessar. Procedimento claro e definido de como os privilégios de acesso são concedidos. Processo definido sobre quem é responsável por autorizar os acessos a dados e registro de tais autorizações. Métodos para análise crítica dos privilégios concedidos e revisão regular dos mesmos.
Gerenciamento de senhas e autenticação	Estabelecer regras para garantir que as senhas e informações de autenticação sejam, e se mantenham, confidenciais. Procedimento para atualizar senhas dos usuários regularmente, bem como, para garantir que sejam fortes o suficiente para não serem descobertas de forma indevida. Registro de que o usuário recebeu as suas informações de autenticação e que o mesmo é responsável por sua confidencialidade e individualidade, através da assinatura de uma declaração para tal.

(conclusão)

Análise dos direitos de acesso	Procedimento que garanta que seja feita análise crítica regularmente dos privilégios de acesso pelos proprietários por grupos de dados e informações. Procedimento que garanta que exista a análise dos privilégios fornecidos sobre acesso de dados em situações específicas, como promoções, alterações de cargos ou mudanças nas divisões de departamentos ou setores da organização.
Exclusão dos direitos de acesso	Procedimento que regule o cancelamento imediato do acesso quando o usuário não mais necessitar, como encerramento do contrato de trabalho, fornecimento de serviço por terceiros ou acesso temporário previamente concedido. Convém que os acessos sejam retirados de maneira imediata, antes da comunicação ao usuário, para que não exista a oportunidade do mesmo coletar informações que possam ser utilizadas de forma futura e indevida.

Fonte: Próprio autor.

Na política de segurança, é preciso que a empresa defina a classificação e o tratamento dos dados em seu poder. Além da informação pertinente as operações da empresa, os dados pessoais em seu poder também devem receber esse tratamento. A informação deve ser classificada em termos de valor, requisitos legais, sensibilidade e criticidade para evitar quebra de segurança. Esse procedimento ajuda a definir como tratar e proteger a informação. A Norma ABNT ISO/IEC 27002 (ABNT, 2013) exemplifica como esquema de classificação a utilização de quatro níveis, com base em uma quebra de confidencialidade: sem danos a organização; com inconveniência operacional baixa; com pequeno impacto significativo nas operações; ou causando sério impacto sobre objetivos estratégicos, operacionais ou mesmo colocando a sobrevivência da organização em risco. Essa classificação, além de estar documentada na política de segurança, deve ser de conhecimento de todos os usuários e envolvidos.

Conforme constatado, a empresa possui um departamento de TI e uma sala fechada que comporta os servidores e equipamentos de armazenamento de dados da empresa. Contudo, não existe documentação que forneça as diretrizes para manter tais departamentos em segurança. Convém que a organização elabore documentação e políticas para manter a segurança física e do ambiente. Tal documentação deve

estabelecer os perímetros de segurança utilizados para proteger não somente as instalações de processamento de dados, como, também, áreas onde informações críticas possam ser encontradas (incluindo dados pessoais).

A empresa conta, atualmente, com uma área de recepção, a qual controla quem entra ou sai da empresa, o que auxilia no controle das instalações da mesma. Internamente, como pôde ser observado em visita realizada na empresa, existe a intenção de substituir o atual local de armazenamento dos dados. A nova instalação para processamento de dados deve ser projetada de forma a proteger os equipamentos de acessos de pessoal não autorizado e, além disso, contra possíveis incidentes que possam ocorrer, como incêndio ou inundação, e ainda contar com sistemas de monitoramento por imagem, trancas que permitam apenas o acesso a pessoal autorizado e alarmes de invasão, diretrizes tais apontadas pela Norma ABNT ISO/IEC 27002 (ABNT, 2013).

O procedimento documentado deve conter as diretrizes que regram quem pode ou não ter acesso às áreas consideradas críticas para segurança da informação e como o acesso é autorizado, formas de informar as áreas consideradas seguras e de responsabilizar os envolvidos pelas atividades que sejam necessárias. O documento também deve dispor de meios para garantir que outras áreas consideradas críticas (como área de RH, áreas de pesquisa de produtos, ambientes que contenham informações delicadas ou sensíveis a organização) também possuam controles que impeçam que os dados possam ser utilizados ou apropriados de forma indevida, tanto de forma lógica ou física. Orienta-se que todos os colaboradores, tanto internos como externos, tenham ciência do valor da informação e dos dados com o qual trabalham, comprometendo-se a manter os mesmos em segurança e não os divulgando a terceiros sem autorização expressa dos proprietários. Termos de responsabilidade e, até mesmo menção a tais cuidados em contratos de trabalho podem ser utilizados como método de reduzir os riscos de informações serem utilizadas de maneira indevida.

Os controles já adotados pela empresa de forma pontual, como sistemas de *firewall, proxy* e IDS, devem possuir uma política documentada que parte desde a forma de contratação e implementação destes controles, sua configuração, a responsabilização dos envolvidos em manter os controles, analisar criticamente os processos adotados.

Deve ser observado que a empresa diz conhecer os riscos e vulnerabilidades que podem atingir a empresa, mas não existe registro sobre esse procedimento. Convém, também, que a empresa estabeleça uma política de análise de riscos, descrevendo os procedimentos para avaliar os ativos de informação da empresa, as ameaças, os controles já existentes, as vulnerabilidades e, então, avaliar os riscos existentes na empresa, bem como o tratamento que deve ser dada a cada um dos riscos.

A empresa Beta conta com sistemas de backups implementados na empresa, mas os procedimentos não são regrados ou seguem uma determinação documentada. Convém que seja criado uma política documentada que determine as regras para realizar os backups. Essas regras devem determinar a periodicidade da realização dos backups e teste de mídias de backup, a responsabilidade pela geração e controle dos backups, consideração do tempo que a empresa pode suportar com a indisponibilidade de dados e informação (caso ocorra um incidente), quais as informações são mais críticas, e maneiras de tratar as mídias e os backups com a confidencialidade a qual se necessita. Deve existir um procedimento regular para testar as mídias geradas e a recuperação dos dados, garantido a confiabilidade no caso de uso emergencial. Também deve ser determinado qual o período de tempo de retenção da informação em backups.

É aconselhável que a empresa tenha uma política de continuidade de negócios implementada, indicando os responsáveis e as ações a serem tomadas se ocorrer um incidente. Esse documento também deve prover o registro dos controles adotados para manter os negócios operantes, como redundância de armazenamento, processamento, energia e links de internet. Esses controles devem ser analisados regularmente, avaliando sua eficácia e garantindo que os sistemas estejam sempre operando conforme as necessidades da empresa.

Após a elaboração e implementação das políticas de controles de segurança, é importante que as mesmas sejam divulgadas a todas as partes envolvidas com o uso de informação e dados da empresa, inclusive partes externas, como representantes e agentes que atuam fora da mesma. Estes devem ser responsáveis por seus atos relacionados a utilização de qualquer recurso de processamento da informação da empresa Beta. Os usuários devem ser instruídos quanto a não deixar mídias, documentos ou equipamentos visíveis que contenham dados pessoais ou

relacionados a empresa, sendo conveniente que meios físicos que contenham tais informações sejam guardados em locais seguros, como cofres ou armários com chaves, que exista limites de utilização de copiadoras, impressoras ou similares, havendo registro do que é impresso e por quem foi impresso. Também convém que os usuários (principalmente os funcionários) assinem algum termo de responsabilidade pela utilização de dados e informações da empresa e, quando cabível, possa ser incorporado a contratos de trabalho ou documentos de contratação, evidenciando as consequências e possíveis penalidades quanto ao uso indevido de informações (se necessário, realizar uma análise jurídica sobre o uso de penalidades válidas no âmbito trabalhista).

Por fim, é aconselhado que a empresa adote medidas de anonimização de dados pessoais quanto utilizados para pesquisa. Se não houver mais a necessidade de relacionar os proprietários com suas informações prestadas, deve-se existir um procedimento que estabeleça regras do que deve ser ainda armazenado (anonimizados) e o que deve ser excluído dos bancos de dados ou mídias de armazenamento, bem como a maneira que esse descarte deve ocorrer.

5.2.3 Análise final – Empresa Beta

Após apreciação das sugestões de melhoria (Apêndice D) pela empresa Beta, uma entrevista com o Gestor da Área de TI da mesma foi realizada, com o objetivo de verificar a percepção quanto as sugestões apresentadas.

Conforme pôde-se verificar, a Empresa Beta avaliou as sugestões apresentadas como válidas, as quais serão melhor analisadas e incluídas no planejamento de projetos da área de TI, os quais devem ser apresentados para a direção para aprovação e apoio futuro. Provavelmente, segundo a organização, essas medidas não serão totalmente adotadas até o momento da entrada em vigor da Lei.

Após a primeira visita realizada na empresa, a mesma passou a apresentar maior preocupação em avaliar os controles de segurança já adotados, realizando testes e análises mais regularmente, o que vem apontando falhas, até então, não percebidas.

Por fim, a empresa também confirma que a direção tem interesse em adotar as melhorias necessárias para manter os dados da empresa e pessoais em segurança, o que ajuda na implementação das melhorias sugeridas.

5.3 CASO 3 – EMPRESA GAMA

A Empresa Gama, organização de direito privado que atua no ramo moveleiro, também foi submetida ao questionário apresentado no Apêndice A, complementado com uma visita para observar os procedimentos adotados pela mesma.

5.3.1 Panorama atual – Empresa Gama

A Empresa Gama demonstrou conhecimento sobre a aprovação da Lei 13.709/18, procurou alternativas para atender aos requisitos, mas não mantém nenhum projeto de adequação à mesma atualmente.

Os dados pessoais em seu poder são armazenados em bancos dedicados, sendo, estes, dados de funcionários, colaboradores e clientes. Os dados são utilizados em processos diversos na organização, não sendo tratados para pesquisas ou geração de dados estatísticos que venham a ser divulgados externamente.

Conforme informado, existe uma política de segurança implementada na empresa, com apoio da direção e divulgada aos colaboradores. Contudo, durante a visita, não foi possível evidenciar a existência de tal documentação. Segundo a empresa, a revisão da política de segurança não é feita de maneira regular, sendo avaliada somente quando há uma necessidade pontual. A avaliação dos riscos iminentes a segurança da informação é realizada de maneira informal, não seguindo procedimentos ou regras estabelecidas.

O controle de acessos é realizado sem que exista um procedimento documentado. As regras adotadas são definidas informalmente, apesar de existir um padrão setorial para realizar a distribuição de acessos e privilégios entre os colaboradores da empresa. O acesso de terceiros e visitantes a organização é controlado, não sendo permitido circular sozinho pela organização, nem utilizar equipamentos que acessam a rede de dados da empresa sem o acompanhamento de um responsável do setor de TI. Além disso, todos as atividades realizadas na rede de dados da empresa são registradas.

O controle de equipamentos utilizados pelos funcionários é realizado pelo setor de Recursos Humanos, o qual é responsável pelo recolhimento desses quando o funcionário encerra suas atividades na empresa. As senhas e os acessos antes liberados também são excluídos quando existe o desligamento do colaborador.

O armazenamento de dados é feito em bancos de dados localizados em uma sala anexa à empresa, construída de forma a ficar isolada das demais instalações. Somente a área de segurança patrimonial da empresa e os colaboradores da TI tem acesso a essa sala. Os computadores possuem softwares antivírus, que são auditados e verificados eventualmente. A empresa também conta com sistemas de detecção de invasão a rede de dados (IDS), *proxy* e *firewall*, proporcionando barreiras para possíveis invasões ou ataques maliciosos.

Existe uma sistemática de backups na empresa, com cópias armazenadas em locais distantes do armazenamento principal da empresa, como também na nuvem. São realizados testes de restauração, avaliando a funcionalidade das mídias e dos *backups*. Contudo, não existe um documento que regule os procedimentos realizados para proteção quanto a perda de dados.

Quando necessário utilizar pontos remotos de trabalho, estes contam com controles de segurança, como utilização de VPNs e criptografia de dados. O acesso realizado pelas franquias ou lojas autorizadas é direcionado somente ao sistema ERP da empresa. Esse acesso é controlado e possui registro das atividades, não sendo possível acessar nenhuma outra base de dados ou discos de armazenamento.

Apesar de existirem redundâncias nos sistemas de informação e armazenamento, não há uma política explícita para garantir a continuidade das operações. Se necessário realizar uma ação em decorrência de um incidente, essa é feita de maneira informal, sem seguir padrões ou planos estabelecidos.

5.3.2 Análise do panorama atual – Empresa Gama

A Empresa Gama demonstrou que procurou esclarecimentos sobre os requisitos impostos pela Lei 13.709/18. Porém, a mesma não buscou levar esse assunto a nível gerencial, não havendo nenhum projeto previsto para adequar processos de forma a atender detalhadamente os requisitos. É aconselhável que a empresa busque maiores detalhes, tanto jurídicos quanto técnicos para atender tanto

os requisitos burocráticos de uso de dados pessoais (consentimento de titulares, por exemplo) quanto requisitos técnicos, que serão apresentados nessa Seção.

A empresa conta com armazenamento e tratamento de dados pessoais de funcionários, alguns fornecedores e clientes. A utilização dos dados é feita dentro das dependências da empresa e por lojas pertencentes à organização. O armazenamento lógico desses dados é feito totalmente nos bancos de dados instalados na empresa.

Como evidenciado, a empresa informa possuir uma política de segurança da informação implementada na empresa, mas não foi evidenciado isso durante a visita realizada. Convém que a mesma busque, primeiramente, o apoio da direção para que se elabore uma política de segurança documentada e coerente com os objetivos da organização, requisitos legais e de contratos vigentes.

A política de segurança da informação deve ser implementada de forma a definir os objetivos de segurança da informação e a abordagem da mesma para gerenciar tais objetivos. Deve atribuir responsabilidades, gerais e específicas, e prover meios para que mesma seja analisada criticamente em períodos regulares, promovendo as alterações pertinentes e garantindo, assim, a melhoria continua dos processos de segurança da informação. Convém que essa política seja de conhecimento de todos os funcionários e envolvidos nos processos que utilizem processamento de informações da empresa, inclusive, com adoção de documentos que registrem os treinamentos direcionados a esses.

A política da segurança deve ser apoiada por políticas de nível mais baixo, direcionadas a procedimentos e controles adotados pela empresa para manter a segurança da informação. Essas políticas são apresentadas no decorrer dessa Seção.

A empresa demonstra adotar controles de acesso, como utilização de credenciais individuais para acesso a dados lógicos, acesso a rede e a sistemas utilizados na empresa, e também existem privilégios de acesso distribuídos para cada usuário. Porém, não existe um procedimento que defina as regras para gerenciar esses controles. Deve ser implementado, portanto, uma política de controle de acesso que detalhe os ativos de informação existentes na empresa, seus devidos proprietários e estes devem definir claramente quais os acessos permitidos a tais ativos. A política de controle de acesso deve levar em consideração os requisitos de negócio da empresa, legislação pertinente e obrigações contratuais, gerenciamento

dos direitos de acesso, responsabilização por pedir, autorizar e administrar os acessos concedidos, análise crítica e periódica dos direitos de acesso, remoção dos direitos de acesso, registro de eventos significantes de acesso e regras para acessos privilegiados.

Com a implementação de uma política de controle de acesso, a empresa pode gerenciar de maneira mais eficaz os controles já existentes, além de prover meios para revisão periódica da mesma e de responsabilização pelo uso dos meios de acesso a informações e dados da organização. Convém que a política seja divulgada a todos usuários (internos e externos), registrando as autorizações de acesso por meio de termos de responsabilidade pelo seu uso, indicando os limites de acesso a cada usuário e possíveis penalizações caso esses limites sejam excedidos ou usados de maneira indevida. As medidas já utilizadas atualmente, como exclusão de acesso e recolhimento de equipamentos de funcionários desligados das atividades da empresa e permissões de acesso a terceiros, por exemplo, devem ser analisadas conforme a política de controle de acesso implementada e incluídas nos termos definidos e documentados.

A Empresa Gama possui seus equipamentos de processamento de informação e armazenamento de dados instalados em uma sala construída para tal, adotando materiais que reduzem a iminência de incidentes como incêndio ou similares. A sala pode ser acessada somente pelo pessoal da TI ou pela área de segurança da empresa. Falta, porém, um procedimento ou política que estipule regras para tal acesso. Uma política de segurança física e de ambiente deve conter a definição das áreas consideradas de risco para a segurança da informação, como a sala de processamento de dados e armazenamento e salas que possuam tratamento de informação sensível a organização. O documento deve estipular quem pode acessar as salas e como esse acesso deve ser feito, bem como a adoção de controles que impeçam que indivíduos não autorizados acessem tais locais. A empresa já conta com uma área de recepção, a qual controla quem acessa as dependências da mesma. A política de segurança física deve ser divulgada a todos os funcionários, os quais devem estar cientes dos cuidados e procedimentos a serem adotados quando trabalham em uma área considerada de segurança, evitando que informações e dados possam ser divulgados ou tratados de forma indevida.

A empresa já adota controles técnicos para proteção dos dados armazenados, como sistemas de *firewall*, *proxy* e IDS. Deve ser elaborada uma política documentada que estipule os procedimentos adotados para implementação, configuração e análises continuas da eficácia desses controles, bem como a responsabilização pelos envolvidos nesses processos. Também convém que se tenha uma política de análise de riscos implementada, com as diretrizes para identificação dos ativos de informação da empresa, as ameaças que rondam esses ativos, as vulnerabilidades que podem ser exploradas e, assim, conhecer os riscos que existem no que diz respeito a segurança da informação. Essa política deve trazer, também, os métodos para se classificar e tratar os riscos, os controles já adotados para tal, e os meios para que se faça uma análise periódica dos riscos e atualização das ações a serem tomadas.

Como existe acesso remoto a sistemas da empresa e transferência de informações e dados entre lojistas e a sede da empresa, convém que se elabore um procedimento documentado, informando os responsáveis pelo gerenciamento dos controles adotados para segurança da rede de dados, os controles utilizados, padrões de configuração, tratamento de exceções e limites de acesso utilizados em trabalhos e acessos remotos.

A Empresa Gama realiza backups de seus arquivos, tanto em mídias físicas quanto na nuvem. As mídias são armazenadas em local separado da origem dos dados. Porém, não existe uma política que defina de forma clara as responsabilidades pela execução, manutenção e testes de backup, e como esses procedimentos devem ser executados. Convém que esse procedimento documentado estipule as definições de tempos e quantidade de dados que devem ser guardados para recuperação em caso emergencial, quais os meios utilizados para realização dos backups, os intervalos entre testes executados, bem como responsáveis pelas ações necessárias em caso de necessidade emergencial de recuperação dos dados.

Os sistemas da Empresa Gama possuem redundância de servidores, sistemas de armazenamento, energia elétrica e comunicação. É recomendado que a mesma elabore uma política de continuidade dos negócios, verificando as necessidades da empresa em quanto tempo ela pode suportar sem seus serviços operantes, e quais os serviços são mais críticos em questão de disponibilidade. Com base nisso, elaborar um documento que defina as ações tomadas para manter os serviços e sistemas de

informação operantes, quais ações são necessárias se ocorrer um incidente, e quem são os responsáveis pelas ações.

Todas as políticas devem ter apoio da direção, a qual deve providenciar que todos usuários possuam conhecimento sobre seu teor e os treinamentos necessários. Estes devem estar cientes dos dados que podem acessar, e sua responsabilidade por esses dados. Instruir os funcionários para não deixar informações a vista de qualquer pessoa, zelando pela segurança tanto de forma lógica quanto física. Além disso, os usuários devem ser responsabilizados pelos meios que utilizam para acesso a informações e dados. A assinatura de termos de responsabilidade é aconselhável, indicando qual a responsabilização do funcionário sobre os sistemas de informação e as cabíveis penalidades, inclusive legais, se algo indevido vier a ocorrer.

5.3.3 Avaliação final – Empresa Gama

A empresa Gama, após a apreciação da proposta de melhoria apresentada no Apêndice E, foi abordada com o objetivo de identificar sua perceptividade quanto ao conteúdo da mesma.

Durante entrevista realizada com o responsável pela área de TI da mesma, pôde-se verificar que as sugestões de melhoria apresentadas foram classificadas como válidas para implementação na empresa. Conforme o entrevistado, a empresa vem buscando maiores informações e detalhes sobre a Lei 13.709/18 no âmbito jurídico, preocupando-se em ter ciência do que é necessário alterar em seus processos para atender os requisitos impostos por esta.

Conforme foi percebido, a empresa considera que os controles de segurança da informação adotados atualmente proporcionam um grau de segurança aceitável, dentro de suas percepções, para manter os dados em segurança. Porém, existe a ciência de que haverá considerável melhoria se forem adotadas as medidas sugeridas como resultado desse trabalho, e que a implementação dessas melhorias demanda empenho e recursos consideráveis para a área de TI e de gestão da empresa.

A preocupação com as adequações necessárias para atender os requisitos da Lei 13.709/18 tem sido observada pela direção da empresa, e as sugestões de melhoria resultantes desse trabalho serão consideradas em projetos que sejam implementados para atender a Lei. De qualquer forma, conforme o entrevistado, a

área de TI da empresa tem interesse, a curto prazo, de implementar políticas coerentes com as sugestões de melhoria apresentadas, e buscará junto a direção da empresa, apoio para tal, independentemente da existência de projetos provenientes da área jurídica sobre a Lei 13.709/18.

5.4 CONSIDERAÇÕES FINAIS

A realização dos estudos de caso para elaboração desse trabalho ocorreu, primeiramente, com a aplicação de um questionário, apresentado no Apêndice A, o qual tinha por objetivo, esclarecer os conhecimentos sobre a Lei 13.709 e os controles e medidas de segurança que cada um dos casos já possuía implementados em suas organizações.

Com base nos resultados desse questionário, foram analisadas as necessidades de adequação para com os requisitos apresentados na Lei 13.709, no que diz respeito a procedimentos técnicos informáticos. As melhorias verificadas foram apresentadas aos casos estudados, conforme os Apêndices C, D e E. Após a apreciação das sugestões de melhoria por parte das empresas, as mesmas foram abordadas quanto a validade de seu conteúdo e se as mesmas poderiam ser consideradas para futura implantação, buscando evidenciar as motivações, tanto negativas quanto positivas, conforme questionário apresentado no Apêndice B.

Com a análise inicial, baseada no questionário aplicado, pôde-se verificar que existe uma diferenciação na estrutura empresarial dos casos estudados, no que diz respeito a gerenciamento de sistemas de informação. As empresas Beta e Gama (empresas de direito privado) possuem uma infraestrutura totalmente gerenciada por pessoal interno, o que não ocorre com a empresa Alfa (empresa de direito público). A empresa Alfa possui gerenciamento da infraestrutura realizado por equipes da Prefeitura de Caxias do Sul, enquanto os sistemas de tratamento e armazenamento de dados pessoais são gerenciados a nível nacional.

Essa constatação, porém, não inibe a empresa Alfa de possuir medidas de segurança da informação. Essas devem ser direcionadas aos processos realizados internamente, onde existe tratamento de informações, juntamente com controles que abordem os serviços realizados por terceiros, com o objetivo de garantir que estes estejam de acordo com os objetivos da empresa em manter a segurança da

informação e dados sensíveis ou críticos aos negócios da mesma. A análise feita após a apreciação das propostas por parte da empresa evidenciou que existe um interesse em implementar medidas eficazes para manter a segurança dos dados, as quais podem ir além das melhorias apresentadas a mesma como parte desse trabalho.

As empresas Beta e Gama, por sua vez, possuem processos bem similares quanto ao tratamento de dados e informações em suas operações. Foi observado que essas já utilizam controles de segurança, como sistemas de segurança de rede e armazenamento (*firewall, proxy systems,* antivírus, utilização de VPNs em acessos remotos e criptografia em transferências de dados) e sistemas de apoio a continuidade dos negócios, como *backups* e redundâncias de equipamentos de armazenamento e processamento de dados.

Apesar da existência de controles de segurança da informação em todos os casos estudados, os mesmos não são implementados ou configurados com base em riscos devidamente analisados ou conhecidos, nem mesmo existem procedimentos padronizados para implementar controles e medidas de segurança.

De forma a atender os requisitos da Lei 13.709 em manter meios técnicos para segurança da informação, em todos os casos estudados existe a necessidade de implementação de políticas de segurança e normas de dimensão que padronizem e regrem a utilização dos controles já adotados atualmente pelas empresas, provendo métodos bem definidos para manter esses controles e atualizá-los conforme as necessidades de negócio ou incidentes e eventos de segurança que possam ocorrer.

6 CONCLUSÃO FINAL

A elaboração deste trabalho se baseou na aprovação da Lei 13.709/18, a qual dispõe de regramento para proteção de dados pessoais em tratamento realizado por empresas, tanto de direito público quanto de direito privado, buscando evidenciar quais ferramentas e medidas técnicas de segurança da informação devem ser adotadas pelas empresas para manter os dados pessoais protegidos.

Primeiramente, uma análise da Lei 13.709/18 foi realizada, observando quais os requisitos técnicos da mesma para, posteriormente, verificar na literatura quais as melhores práticas em segurança da informação deveriam ser implementadas pelas empresas para atender os requisitos da Lei.

Um estudo de caso foi realizado, então, em três organizações, buscando evidenciar quais os controles estas já possuíam, em relação a segurança da informação, e quais as melhorias em seus processos deveriam ser realizadas para atender os requisitos da Lei 13.709. Esse estudo ocorreu por meio da aplicação de um questionário de pesquisa (Apêndice A), que buscou o conhecimento da atual situação dos casos estudados, análise dos resultados, comparando as medidas já adotadas com as necessidades impostas pela Lei 13.709/18, elaboração de propostas de melhorias (Apêndices C, D e E) para cada um dos casos e verificação, com gestores de cada uma das empresas, sobre a aceitação das sugestões de melhoria apresentadas.

Analisando a Lei 13.709/18, pôde-se verificar que a mesma pode ser dividida em dois objetivos, considerando a abordagem de métodos de proteção aos dados pessoais impostos por ela: proteção aos titulares de dados pessoais; e regramento de segurança da informação e governança para as empresas que realizam tratamento de dados pessoais.

Para realizar a proteção aos titulares dos dados, a Lei apresenta regras que partem do consentimento dos titulares para coleta, tratamento, armazenamento e eliminação de dados pessoais. Além dessas, são observadas regras para que as empresas mantenham registros e informações da situação que os dados pessoais se encontram, como também dos direitos que os titulares têm sobre obter informações das empresas quanto a esses dados e o que pode ser solicitado e deve ser atendido prontamente pelas empresas que tem os dados sob sua guarda. São apresentadas,

também, as exceções em que o titular não necessita, obrigatoriamente, permitir que haja o tratamento ou armazenamento de seus dados pessoais.

No que diz respeito aos requisitos técnicos informáticos impostos pela Lei 13.709/18, pôde-se verificar que é devido as empresas manter medidas e controles de segurança da informação que inibam o acesso indevido ou mal-intencionado aos dados pessoais em seu poder. As medidas e controles a serem adotados não são especificados diretamente. A Lei menciona em quais processos de tratamento de dados deve existir algum ponto de controle de segurança, como transmissão de dados, armazenamento, ações para contingência de quebra de segurança ou indisponibilidade dos dados, procedimentos para controle de acesso, divulgação, tratamento, alteração ou exclusão indevidos dos dados pessoais em seu poder.

Partindo dos requisitos técnicos de proteção de dados apresentados na Lei 13.709/18 e analisando literatura pertinente a segurança da informação, além de normas em vigor no Brasil, identificou-se que as empresas devem possuir medidas e controles implementados para garantir:

a) a transmissão segura dos dados;

b) o controles de acesso aos dados;

c) a proteção contra vazamento de dados;

d) a proteção à integridade dos dados;

e) a proteção quanto a perda indevida dos dados;

f) a garantia de disponibilidade dos dados;

g) o gerenciamento da segurança dos dados.

Incluídos a esses pontos de segurança, a Lei também solicita que existam procedimentos ou planos de ações documentados para caso ocorra algum incidente que envolva a quebra de confidencialidade ou integridade dos dados pessoais em poder das empresas.

Identificados os pontos de controle que devem ser observados pelas organizações, pôde-se evidenciar as melhores medidas e controles de segurança a serem adotados. Resumidamente, a adoção dos processos de segurança

apresentados nas normas ABNT ISO/IEC da série 27000, que dispõe sobre as melhores práticas para se criar um sistema de gerenciamento de segurança da informação para qualquer organização, se mostra suficiente para que se atendam aos requisitos técnicos de segurança apresentados na Lei 13.709/18.

Portanto, é conclusivo afirmar que o atendimento aos requisitos técnicos informáticos de segurança da Lei 13.709/18 parte da adoção de um sistema de segurança da informação, com a devida identificação e análise dos riscos iminentes aos dados e informações, tanto pessoais quanto da própria organização. Com base nesse procedimento, a implementação de uma política de segurança devidamente documentada, tomando por base a Norma ABNT ISO/IEC 27002:2013 (ABNT, 2013), e o apoio de normas e políticas de dimensão, padronizando a adoção de controles e medidas para reduzir ou eliminar os riscos de quebra de segurança identificados na organização. Na elaboração das políticas e normas de dimensão, devem existir planos ou procedimentos que definam as ações para conter os possíveis prejuízos causados por uma quebra de segurança, bem como meios de informar aos titulares dos dados os danos causados e as medidas adotadas para contornar um incidente de segurança.

A adoção desses procedimentos e políticas de segurança confere à organização não somente um meio de atender aos requisitos da Lei 13.709/18, mas, também, um sistema completo e definido de responsabilidades e ações para manter toda a informação sensível da organização em segurança. Isso permite que exista o controle sobre a continuidade das operações da empresa e a redução de prejuízos na ocorrência de um incidente que possa atingir os sistemas de informação da empresa. Muitas vezes, falhas na avaliação de riscos ou a falta de padrões e procedimentos específicos para se analisar e avaliar quais os riscos e os meios para contorna-los só são percebidos na ocorrência de um incidente que, dependendo da sua magnitude, pode causar prejuízos consideráveis para uma organização, independentemente do seu porte ou tipo de operação.

Com base na análise referente aos requisitos técnicos da Lei 13.709/18, foram estipulados três estudos de caso para realizar sua validação. A seleção dos casos a serem estudados para validação procurou identificar os processos de empresas privadas e de direito público. Uma das organizações (Empresa Alfa) é uma empresa de direito público, que realiza atendimento de público a nível regional e possui coleta e tratamento constante de dados pessoais. Os outros dois casos (Empresa Beta e

Empresa Gama) são empresas de direito privado, representando processos comuns de grande parte das organizações inseridas na região de Caxias do Sul.

A coleta inicial de dados dessas organizações procurou perceber, primeiramente, qual a ciência das mesmas quanto a aprovação da Lei 13.709/18 e quais as medidas que as mesmas haviam tomado para se adequar aos seus requisitos. Os três casos estudados apresentaram preocupação em como deveriam adotar medidas ou mudar processos para que pudessem atender os requisitos da Lei, procurando auxílio jurídico em todos os casos. Contudo, somente a empresa Alfa procurou implementar projetos ou ações para adequar processos internos que visassem atender aos requisitos da Lei, ou, de alguma forma, incluir os assuntos e requisitos abordados na Lei 13.709/18 em projetos novos ou já em andamento. Os outros dois casos, como foi percebido, buscaram apenas se informar sobre os requisitos, mas não possuem projetos ou planejamento de adoção de medidas que possam adequar seus processos aos requisitos impostos pela Lei, aceitando que possam existir falhas em seus processos, as quais podem ser contornadas com os controles já existentes e implementados em seus processos.

Ao analisar as informações prestadas pelas organizações no que diz respeito aos controles já adotados, percebeu-se que estas adotam controles pontuais de segurança em seus processos. Esses controles, porém, são selecionados, implementados e utilizados sem haver uma análise prévia concisa. Nos casos das empresas Beta e Gama, foi percebido que a adoção e configuração dos controles de segurança é bastante informal, realizada a partir de incidentes que ocorrem com outras organizações ou eventos cotidianos de tentativas de quebra de segurança que acontecem nas próprias empresas. A empresa Alfa, por sua vez, possui o gerenciamento de sua infraestrutura de TI realizado pela Prefeitura de Caxias do Sul, não existindo, até então, um controle por parte dessa para determinar quais os controles de segurança que podem ser implementados em seus sistemas de informação lógicos.

Como não existe um processo de avaliação de riscos implementado em nenhuma das organizações, a realização da seleção dos controles é, de certa forma, falha. Um sistema de segurança da informação, que confere segurança também aos dados pessoais em poder das organizações, deve se basear na análise dos riscos iminentes aos sistemas de informação destas, tanto de forma lógica quanto física.

Como em nenhum dos casos esse processo é feito de forma padronizada, com uma política ou procedimento documentado, a definição dos demais componentes de segurança da informação também é falha.

Partindo dessa constatação, e com base nas medidas e mecanismos de segurança necessários para se atender os requisitos, é evidente que as organizações precisam implementar um procedimento consistente para identificar, analisar e propor o devido tratamento aos riscos iminentes para a segurança da informação. Essa análise, se bem realizada (aconselha-se tomar como referência a Norma ABNT ISO/IEC 27005), confere o conhecimento prévio dos possíveis incidentes que podem ocorrer aos sistemas de informação da empresa, auxiliando, de forma coerente, à seleção dos controles e medidas de segurança que devem ser implementados para reduzir os riscos a um nível aceitável e desejado pela organização, dentro de seus objetivos e estratégias de negócio e as normas e legislação vigente (inclusive, a Lei 13.709/18).

Baseada nos riscos devidamente analisados, a adoção de controles e medidas de segurança, bem como sua configuração e utilização, é mais eficaz para manter a segurança da informação em uma organização. Nos casos estudados, os controles adotados são considerados, pelas próprias empresas, suficientes para manter a segurança dos dados e informações em seu poder. Em partes, sim, esses controles podem ser eficientes para atender a demanda de segurança necessária. Porém, estes podem apresentar lacunas (e provavelmente apresentem) para que ameaças possam atingir os sistemas de informação ali presentes, inclusive dados pessoais. Incluem-se, aqui, controles como dispositivos de segurança para armazenamento e rede (*firewall, proxy systems*, procedimentos de controle de acesso como senhas e permissões de acesso, programas antivírus, definições de privilégios de acesso), cópias de segurança, redundância de sistemas (canais de comunicação e internet, energia, armazenamento e processamento de informações) e controles físicos de segurança de ambiente (controles de acessos a departamentos, definição de áreas de segurança). Não há como garantir que os controles e procedimentos já adotados pelas organizações efetuem uma segurança satisfatória para os dados e informações em seu poder se não existe um padrão ou procedimento que estipule as regras ou ações a se tomar (inclusive os responsáveis por tais ações) para que exista, de fato, a segurança conforme objetivos estabelecidos para tal.

Portanto, a maneira para atender os requisitos técnicos de segurança estabelecidos pela Lei 13.709/18 e a informação crítica e sensível organizacional para os casos estudados (podendo-se estender a outras organizações), é a adoção de um procedimento documentado para conhecimento e análise de riscos à segurança da informação, implementação de uma Política de Segurança da Informação (PSI) baseada nos riscos e nos objetivos da organização (a qual deve ser de conhecimento de toda a organização e ter a aprovação e o apoio da direção) e implementação de políticas de apoio e normas de dimensão que padronizem os controles adotados em observação aos requisitos e objetivos propostos na PSI.

A adoção de procedimentos e políticas que regrem os controles adotados pelos casos estudados garante que se saiba as ações a serem tomadas na ocorrência de um incidente, como também o conhecimento e a responsabilização de todos os envolvidos para que se mantenha a segurança da informação dentro da organização, reduzindo, assim, os prejuízos decorrentes de um incidente. Também fica claro o papel e a responsabilização dos usuários e funcionários no que diz respeito a segurança da informação, proporcionando que todos conheçam a importância de manter a segurança da informação nas suas tarefas cotidianas, inclusive, de dados pessoais que possam estar envolvidos nessas tarefas.

O caso da empresa Alfa apresenta um ponto de vista diferente, considerando que suas operações não incluem o gerenciamento de infraestrutura e sistemas de Tecnologia da Informação. Isso, porém, não a isenta de implementar um procedimento documentado para análise de riscos de segurança da informação, uma PSI que atente aos seus objetivos como organização e os riscos presentes, e políticas e normas específicas para garantir a segurança da informação e dados pertinentes as suas operações (principalmente, no caso desse trabalho, pela quantidade expressiva de dados pessoais que circulam pelos processos executados na empresa). Os procedimentos e medidas a serem adotados devem considerar não somente os processos internos da organização, mas se estender aos serviços executados por terceiros dentro da organização, através de políticas de segurança voltadas a contratação e solicitação de serviços externos e métodos de responsabilização desses agentes por manter a segurança da informação durante a prestação de serviços ou fornecimento de produtos e sistemas.

Em resumo, nos três casos estudados, existe a necessidade de se analisar os reais riscos iminentes a organização, através de procedimentos padronizados e estabelecidos, uma vez que em nenhum dos casos existe tal análise. Aliado a isso, nos três casos também devem ser implementadas políticas que gerenciem os controles e medidas de segurança utilizados nas empresas, definindo os responsáveis pelas ações que devem ser tomadas para manter esses controles e no caso de ocorrer um incidente. A providência de tais ações, juntamente com os controles já adotados pelas empresas, adere aos requisitos técnicos que foram apresentados nesse trabalho para atender a Lei 13.709/18.

A análise dos requisitos técnicos realizada proporcionou a criação de sugestões de melhorias específicas para cada caso estudado. Essas sugestões foram apresentadas às empresas, as quais puderam apreciá-las e analisa-las. Em decorrência dessa análise, as empresas foram abordadas com o objetivo de verificar sua posição quanto a validade de implementação das sugestões apresentadas.

Entre os três casos estudados, observou-se que cada uma das organizações apresentou um ponto de vista diferente quanto a aceitação das sugestões de melhorias. No caso da empresa Alfa, houve uma aceitação plena e um interesse em evoluir na implementação de medidas coerentes com as sugestões de melhorias apresentadas. A empresa Beta demonstrou conhecer a necessidade da implementação de políticas e normas de segurança em sua organização, mas não pretende realizar a curto prazo a implementação dessas, devido à falta de recursos e pessoal para tal. A empresa Gama, por sua vez, acredita que os controles que a mesma utiliza atualmente já são satisfatórios para atender seus objetivos, mas também não descarta a implementação das melhorias sugeridas, juntamente com outros projetos de adequação para atender a Lei 13.709/18.

Pôde-se perceber que a empresa Alfa tomou tal percepção quanto as sugestões apresentadas pelo teor das operações realizadas pela mesma. A empresa trata de dados pessoais e sensíveis do público em geral diariamente, e possui ciência do teor jurídico apresentado pela Lei 13.709/18, além de outras regulamentações vigentes que devem ser observadas para que se tenha total cuidado com os dados e informação que a mesma trata em suas operações. Essa preocupação, em conjunto com a observância constante das penalizações cabíveis ao não atendimento dos requisitos apresentados na Lei, proporciona uma atenção maior na tomada de ações

que possam prevenir o acesso indevido e não autorizado à informação que a mesma possui em seus sistemas e departamentos.

Nos casos das empresas Beta e Gama, verifica-se que as empresas de direito privado possuem foco maior em suas operações, procurando manter, principalmente, informações sensíveis aos negócios das mesmas em segurança. Não que não exista preocupação em manter dados pessoais em segurança dentro da organização. Mas, provavelmente por falta de maturidade em seus departamentos de TI, juntamente com planos estratégicos e objetivos da alta direção, em prover recursos para que se implemente políticas de segurança aderentes ao negócio e processos da empresa, os quais atendem os requisitos técnicos impostos pela Lei 13.709/18.

Também se observa que a inexistência de um processo de análise de riscos implementado e coerente com os negócios e objetivos das empresas condiciona a escolha e configuração de controles de segurança que podem ser falhos, dependendo da ameaça que vier a atingir os ativos de informação da empresa. As empresas devem ter conhecimento de todos os riscos iminentes a informação, para que, assim, possam definir as melhores medidas para manter a segurança da informação em suas organizações. Porém, nem sempre isso é atentado quando se tomam ações para definir controles de segurança da informação. Uma avaliação consistente dos riscos pode evidenciar ameaças ou vulnerabilidades que, muitas vezes, só serão percebidas na ocorrência de um incidente futuro.

Uma das premissas que foi evidenciada durante as análises feitas foi que as empresas estudadas acreditam que problemas de vazamento de dados ocorrem somente em organizações de grande porte, multinacionais ou similares, e que os prejuízos decorrentes desses vazamentos são consideráveis somente em organizações desse porte. Isso também serve como justificativa para que não exista um esforço ou provimento de recursos para que se implementem políticas e procedimentos documentados conforme os apresentados nas sugestões de melhoria.

É necessário que as organizações atentem as possíveis consequências de um incidente de segurança da informação, provendo recursos e incluindo em suas estratégias e objetivos, a segurança da informação como um todo, inclusive, dos dados pessoais em seu poder. Isso evita que a devida importância à segurança da informação venha a ser percebida somente na ocorrência de um incidente, onde os

custos para contornar os prejuízos podem ser maiores que o necessário para se implementar um Sistema de Segurança da Informação bem documentado, com as ações e responsabilidades bem definidas conforme análises consistentes dos riscos iminentes e coerentes com os objetivos destas organizações.

Como contribuição, o questionário utilizado neste trabalho (Apêndice A) pode ser utilizado, de forma geral, como um guia de diagnóstico quanto aos principais controles de segurança da informação que podem ser implantados em uma empresa para atender os requisitos da Lei 13.709/18.

Sugere-se, como continuidade ou complementação da realização desse trabalho: pesquisas a ações públicas que estão sendo desenvolvidas a fim de divulgar os requisitos da Lei 13.709/18 e sua eficácia relacionada a requisitos técnicos da mesma; a aderência da Norma ISO/IEC 29100 aos requisitos impostos pela Lei 13.709/18; e estudos de caso fundamentados em requisitos técnicos informáticos de ações penais com base na Lei 13.709/18 (atentando a permissão legal para tal).

REFERÊNCIAS

ANTON, Eric Ricardo. Redes de Computadores I. 1999. Disponível em: <https://www.gta.ufrj.br/grad/99_2/eric/index.htm#IPv6>. Acesso em: 16 nov. 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001:2013: Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos. Rio de Janeiro, 2013.

_____. NBR ISO/IEC 27002:2013: Tecnologia da Informação - Técnicas de segurança - Código de prática para gestão da segurança da informação. Rio de Janeiro: Abnt, 2013.

_____. **NBR ISO/IEC 27003:2011**: Tecnologia da Informação - Técnicas de segurança - Diretrizes para implantação de um sistema de gestão da segurança da informação. Rio de Janeiro, 2011.

_____. **NBR** ISO/IEC 27004:2010: Tecnologia da informação - Técnicas de segurança - Gestão da segurança da informação - Medição. Rio de Janeiro, 2010.

_____. **NBR ISO/IEC 27005:2008**: Tecnologia da Informação - Técnicas de segurança - Gestão de riscos de segurança da informação. Rio de Janeiro, 2008.

BASTOS, Luís Othon. **A mentoria na sucessão familiar e a perenidade das empresas - casos de sucesso.** 2006. 118 f. Dissertação (Mestrado) - Curso de Administração, Programa de Pós-Graduação em Administração, Universidade Federal de Pernambuco, Recife, 2006. Disponível em: <https://repositorio.ufpe.br/bitstream/123456789/978/1/arquivo1310_1.pdf>. Acesso em: 16 nov. 2018.

BRASIL, Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União. Brasília, DF, 15 ago, 2018. Seção 1. pt. 59.

CARISSIMI, Alexandre da Silva; ROCHOL, Juergen; ZAMBENEDETTI, Lisandro. **Redes de computadores.** Porto Alegre: Bookman, 2009.

COMISSÃO EUROPEIA (Bélgica). **Proteção de dados:** Regras para a proteção de dados pessoais dentro e fora da UE. 2018. Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection_pt>. Acesso em: 16 nov. 2018.

COMPUTER WORLD (Brasil). **Vazamentos de dados pessoais na deepweb atingem cerca de 50 milhões de usuários.**2016. Disponível em: <https://computerworld.com.br/2016/10/28/vazamentos-de-dados-pessoais-na-deepweb-atingem-cerca-de-50-milhoes-de-usuarios/>. Acesso em: 06 set. 2018.

COMPUTER WORLD (Brasil). **Ransomware volta a ganhar força e ataques crescem 229%.** 2018. Disponível em: <https://computerworld.com.br/2018/07/19/ransomware-volta-a-ganhar-forca-e-ataques-crescem-229/>. Acesso em: 15 set. 2018.

COMPUTER WORLD (Brasil). **Em meio a grandes escândalos, segurança de dados é peça-chave para empresas.**2018. Disponível em: <https://computerworld.com.br/2018/04/17/em-meio-grandes-escandalos-seguranca-de-dados-e-peca-chave-para-empresas/>. Acesso em: 15 set. 2018.

CRESWELL, John W. **Projeto de pesquisa:** Métodos qualitativo, quantitativo e misto. 3. ed. Porto Alegre: Artmed Editora S.a., 2010.

EXAME (Brasil). **Zuckerberg admite necessidade de regulação das redes sociais.** 2018. Disponível em: <https://exame.abril.com.br/tecnologia/zuckerberg-admite-necessidade-de-regulacao-das-redes-sociais/>. Acesso em: 12 set. 2018.

FONTES, Eduardo. **Segurança da Informação:** O usuário faz a diferença. São Paulo: Saraiva, 2006.

FOROUZAN, Behrouz A.; MOSHARRAF, Firouz. **Redes de computadores:** Uma abordagem top-down. Porto Alegre: Amgh, 2013.

GALVÃO, Michele da Costa (Org.). **Fundamentos em Segurança da Informação.** São Paulo: Pearson Education do Brasil, 2015.

GIL, Antonio Carlos. **Estudo de caso.** São Paulo: Ed. Atlas S.A., 2009.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social.** 6. ed. São Paulo: Atlas, 2008.

GOODRICH, Michal T.; TAMASSIA, Roberto. **Introdução à segurança de computadores.** Porto Alegre: Bookman, 2013.

HINTZBERGEN, Jule et al. **Fundamentos de segurança da informação:** com base na ISO 27001 e ISO 27002. Rio de Janeiro: Brasport Livros e Multimídia, 2018.

IBM NEWS ROOM (New York). **Ponemon Institute Cost of a Data Breach Study 2018.** 2018. Disponível em: <https://securityintelligence.com/series/ponemon-institute-cost-of-a-data-breach-2018/?mhq=2018%20ponemon&mhsrc=ibmsearch_a>. Acesso em: 16 nov. 2018.

KIM, David; SOLOMON, Michael G.. **Fundamentos de segurança de sistemas de informação.** Rio de Janeiro: Ltc, 2014.

KUROSE, James F.; ROSS, Keith W.. **Redes de computadores:** uma abordagem top-down. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

MARTINS, Gilberto de Andrade. **Estudo de caso:** Uma estratégia de pesquisa. 2. ed. São Paulo: Ed. Atlas S.a., 2008.

MEDEIROS, Gillyane. **GESTÃO DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO DOS INSTITUTOS FEDERAIS DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA.** 2016. 46 f. TCC (Graduação) - Curso de Tecnologia em Redes de Computadores, Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, Natal, 2016.

NAVARRO, Ana Maria Neves de Paiva. **O direito fundamental à autodeterminação informativa.**2011. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=86a2f353e1e6692c>. Acesso em: 18 nov. 2018.

OLIVEIRA, Wilson José de. **Segurança da Informação:** Técnicas e soluções. Florianópolis: Visual Books Ltda, 2001.

OLIVEIRA, Wilson. **Técnicas para hackers e soluções para segurança:** versão 2. Lisboa: Centro Atlântico, 2003. 602 p.

PESSOA, Raimundo Alan Matos. **UM ESTUDO DE CASO SOBRE A GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM UMA INSTITUIÇÃO FINANCEIRA.** 2012. 58 f. TCC (Graduação) - Curso de Ciências da Computação, Departamento de Ciências Exatas, Universidade Estadual do Sudoeste da Bahia, Vitória da Conquista, 2012.

PONEMON INSTITUTE (Estados Unidos). **2018 Cost of a Data Breach Study:** Global Overview. Michigan: S.n., 2018.

SÃO PAULO. Nucleo de Informação e Coordenação do Ponto Br. Comitê Gestor da Internet no Brasil. **Segurança em IPv6.** 2012. Disponível em: <ftp://ftp.registro.br/pub/gter/gter33/Tutorial-IPv6-Seguranca.pdf>. Acesso em: 16 nov. 2018.

SCHIER, Inara. **Empreendedorismo:** Uma análise sobre o desenvolvimento de empresas brasileiras do setor de software. 2009. 110 f. Dissertação (Mestrado) - Curso de Administração, Programa de Pós-Graduação em Administração, Universidade do Vale do Rio dos Sinos, São Leopoldo, 2009. Disponível em: <http://biblioteca.asav.org.br/vinculos/tede/InaraSchierAdministracao.pdf>. Acesso em: 16 nov. 2018.

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

STALLINGS, William. **Network security essentials:** Applications and standards. 4. ed. Upper Saddle River: Pearson Education, 2011.

TANENBAUM, Andrew S.; WETHERALL, David. **Redes de computadores.** 5. ed. São Paulo: Pearson Prentice Hall, 2011.

TECMUNDO (Brasil). **GDPR: a nova lei cibernética que pode afetar todo o mundo.** 2018. Disponível em: <https://www.tecmundo.com.br/seguranca/128537-gdpr-nova-lei-cibernetica-afetar-mundo.htm>. Acesso em: 12 set. 2018.

VIEIRA, Sonia. **Como elaborar questionários.** São Paulo: Atlas, 2009.

YIN, Robert K.. **Estudo de caso:** Planejamento e métodos. 5. ed. Porto Alegre: Bookman, 2015.

ZANELLA, Tatieli. **Estudo sobre a quebra de confidencialidade da informação e mecanismos de segurança.** 2017. 69 f. TCC (Graduação) - Curso de Sistemas de Informação, CCET, Universidade de Caxias do Sul, Caxias do Sul, 2017.

APÊNDICE A – QUESTIONÁRIO SOBRE REQUISITOS DA LEI E SITUAÇÃO ATUAL DA EMPRESA

O questionário deve ser respondido em sua totalidade, e tem o objetivo de ver claramente como está a questão da segurança da informação na organização, além da percepção do entendimento da aprovação da Lei 13.709, que trata da proteção de dados pessoais.

Seção 1 - Percepções sobre a Lei 13.709/18

As perguntas 1 a 5 têm o objetivo de identificar qual a percepção da empresa quanto à aprovação da Lei 13.709 e quais as tratativas em andamento para buscar atender os requisitos impostos pela mesma.

1. A empresa possui ciência da aprovação da Lei 13.709/18, que dispões sobre os regramentos sobre tratamento de dados pessoais?
( ) Sim
( ) Não
( ) Não sei responder

2. A aprovação da Lei 13.709 já entrou em pauta em alguma reunião gerencial da empresa?
( ) Sim
( ) Não
( ) Não sei responder

3. A empresa, de alguma forma, já procurou compreender os requisitos impostos pela Lei 13.709?
( ) Sim
( ) Não
( ) Não sei responder

4. A empresa já procurou alguma alternativa para atender aos requisitos impostos pela Lei 13.709?
( ) Sim
( ) Não
( ) Não sei responder

5. Existe algum projeto em andamento na empresa com o objetivo de atender os requisitos impostos pela Lei 13.709?
( ) Sim
( ) Não
( ) Não sei responder

Seção 2 - Dados pessoais em poder da empresa

As perguntas 6 a 13 têm o objetivo de identificar a percepção da empresa quanto aos dados pessoais em seu poder e como estes dados são tratados em relação à Segurança da Informação.

6. Como os dados pessoais de funcionários são armazenados pela empresa?
( ) Em papel
( ) Em bancos de dados dedicados
( ) Em arquivos eletrônicos (Word ou Excel, por exemplo)
( ) Não existe armazenamento destes dados

7. Como os dados pessoais de clientes são armazenados pela empresa?
( ) Em papel
( ) Em bancos de dados dedicados
( ) Em arquivos eletrônicos (Word ou Excel, por exemplo)
( ) Não existe armazenamento destes dados

8. Como os dados pessoais de fornecedores são armazenados pela empresa?
( ) Em papel
( ) Em bancos de dados dedicados
( ) Em arquivos eletrônicos (Word ou Excel, por exemplo)
( ) Não existe armazenamento destes dados

9. Como os dados pessoais de público em geral são armazenados pela empresa?
( ) Em papel
( ) Em bancos de dados dedicados
( ) Em arquivos eletrônicos (Word ou Excel, por exemplo)
( ) Não existe armazenamento destes dados

10. Após a utilização dos dados pessoais em poder da empresa, os mesmos são eliminados, de maneira a não poderem mais ser utilizados?
( ) Sim
( ) Não

11. A empresa utiliza dados de clientes ou público em geral para gerar dados estatísticos ou para fins de pesquisa?
( ) Sim
( ) Não

12. Existe alguma maneira de relacionar os dados apresentados em pesquisas ou estatísticas com seus titulares?
( ) Sim
( ) Não
( ) Não se aplica

13. A empresa utiliza de formulários em sites da Internet para obter dados de clientes ou público em geral?
( ) Sim
( ) Não

Seção 3 - Sistemas de informação - Gestão da segurança da informação

As perguntas 14 a 19 têm o objetivo de identificar a atual situação da empresa quanto ao gerenciamento da segurança da informação.

14. Existe uma política de segurança da informação implementada na empresa?
( ) Sim
( ) Não
( ) Não sei responder

15. A política de segurança da informação tem apoio e comprometimento da direção?
( ) Sim
( ) Não
( ) Não sei responder

16. A política de segurança da informação é divulgada e comunicada a todos colaboradores?
( ) Sim
( ) Não
( ) Não sei responder

17. A política de segurança da informação é revisada regularmente, com a realização das correções e alterações, conforme necessidades verificadas?
( ) Sim
( ) Não
( ) Não sei responder

18. Existe a avaliação de riscos e ameaças regularmente, com o objetivo de melhorar a segurança da informação na organização?
( ) Sim
( ) Não
( ) Não sei responder

Seção 4 - Medidas e ferramentas de segurança da informação

As perguntas a seguir têm o objetivo de identificar quais as medidas e ferramentas adotadas pela empresa para manter a segurança da informação.

- As questões 19 a 32 têm a finalidade de evidenciar as medidas referentes ao controle de acessos aos sistemas de informação da empresa;
- As questões 33 a 46 têm a finalidade de evidenciar as medidas adotadas para garantir o armazenamento seguro dos dados;
- As questões 47 a 49 têm o objetivo de identificar as medidas adotadas no que diz respeito à proteção quanto a perda de dados;
- As questões 50 a 53 têm a finalidade de evidenciar as medidas adotadas para garantir a transmissão segura dos dados;
- As questões 54 a 58 têm o objetivo de identificar as medidas adotadas para garantir a disponibilidade dos dados pela organização.

19. Existem políticas documentadas de controle de acessos na empresa?
( ) Sim
( ) Não
( ) Não sei responder

20. Existem políticas documentadas para uso dos sistemas descritos abaixo? (Pode existir mais de uma resposta)
( ) Internet
( ) E-mail ou correio eletrônico
( ) Computadores e outros dispositivos informáticos
( ) Nenhum dos anteriores
( ) Não sei responder

21. Existem políticas de acesso a salas de servidores ou bancos de dados na empresa?
( ) Sim
( ) Não
( ) Não sei responder

22. Os funcionários estão instruídos quanto as suas responsabilidades e deveres em relação à utilização de sistemas de informação na empresa?
( ) Sim
( ) Não
( ) Não sei responder

23. Existe controle de fornecedores que circulam dentro das dependências da empresa?
( ) Sim
( ) Não
( ) Não sei responder

24. Existe controle de visitantes que circulam dentro das dependências da empresa?
( ) Sim
( ) Não
( ) Não sei responder

25. Quando um funcionário ou fornecedor encerra suas atividades na empresa, seus direitos de acesso a sistemas de informação são excluídos?
( ) Sim
( ) Não
( ) Não sei responder

26. O visitante circula pelas dependências da empresa sozinho?
( ) Sim
( ) Não
( ) Não sei responder

27. Existe um perímetro de segurança claramente definido para a área de TI?
( ) Sim
( ) Não
( ) Não sei responder

28. Existem mecanismos de controle, como trancas ou senhas, para acesso à área de TI?
( ) Sim
( ) Não
( ) Não sei responder

29. Existe sistema de monitoramento por câmeras nas dependências da empresa?
( ) Sim
( ) Não
( ) Não sei responder

30. Existem logs sobre as atividades efetuadas na rede da empresa?
( ) Sim
( ) Não
( ) Não sei responder

31. As senhas de acesso são alteradas periodicamente?
( ) Sim
( ) Não
( ) Não sei responder

32. Visitantes, fornecedores ou terceiros possuem acesso à rede da empresa?
( ) Sim
( ) Não
( ) Não sei responder

33. No caso em que um funcionário, fornecedor ou terceiro use seu próprio equipamento, existe um procedimento para assegurar que toda a informação relevante seja transferida para a organização e que seja apagada de forma segura do equipamento?
( ) Sim
( ) Não
( ) Não sei responder

34. Existem políticas para uso de dispositivos pessoais na empresa, como *smartphones, tablets, notebooks* ou similares?
( ) Sim
( ) Não
( ) Não sei responder

35. Existe um processo formal para a devolução de todos os equipamentos, documentos corporativos, *softwares*, dispositivos de computação móvel, cartões de crédito, cartões de acesso, manuais e informações armazenada sem mídia eletrônica entregues a pessoa que está encerrando suas atividades na empresa?
( ) Sim
( ) Não
( ) Não sei responder

36. É possível utilizar dispositivos de armazenamento nos computadores da empresa, como *pen-drives* ou cartões de memória?
( ) Sim
( ) Não
( ) Não sei responder

37. Os usuários podem instalar *softwares* nos computadores da empresa
( ) Sim
( ) Não
( ) Não sei responder

38. Existem perfis diferentes de acesso, com diferentes privilégios, aos sistemas de informação da empresa?
( ) Sim
( ) Não
( ) Não sei responder

39. O controle de privilégios quanto ao acesso aos sistemas de informação da empresa é constantemente revisado e alterado, conforme as políticas de acesso de cada funcionário?
( ) Sim
( ) Não
( ) Não sei responder

40. Os usuários podem alterar configurações em seus computadores?
( ) Sim
( ) Não
( ) Não sei responder

41. Os computadores são regularmente auditados para verificar se existem softwares não autorizados instalados nos mesmos? Existem programas antivírus instalados nos mesmos?
( ) Sim
( ) Não
( ) Não sei responder

42. Existe a possibilidade de trabalho remoto na empresa?
( ) Sim
( ) Não
( ) Não sei responder

43. Existe um sistema de Firewall instalado na rede da empresa, com regras bem definidas e implementadas?
( ) Sim
( ) Não
( ) Não sei responder

44. Existe algum sistema de detecção de invasão à rede da empresa (IDS)?
( ) Sim
( ) Não
( ) Não sei responder

45. Existe algum serviço de Proxy instalado na rede da empresa para o acesso à internet?
( ) Sim
( ) Não
( ) Não sei responder

46. Os acessos à internet efetuados pelos funcionários são registrados e controlados?
( ) Sim
( ) Não
( ) Não sei responder

47. Existe política de backup implementada na empresa?
( ) Sim
( ) Não
( ) Não sei responder

48. As mídias geradas no backup são restauradas periodicamente para testar sua funcionalidade?
( ) Sim
( ) Não
( ) Não sei responder

49. As cópias são armazenadas em local distante do local de armazenamento principal?
( ) Sim
( ) Não
( ) Não sei responder

50. A utilização de pontos remotos de trabalho contempla ferramentas de criptografia na transmissão de dados?
( ) Sim
( ) Não
( ) Não sei responder

51. A transmissão remota de dados utiliza VPN?
( ) Sim
( ) Não
( ) Não sei responder

52. Existem sistemas de proteção de e-mail, como criptografia de mensagens, PGP ou similares?
( ) Sim
( ) Não
( ) Não sei responder

53. Quando redes públicas são utilizadas para transmissão de dados, existe a preocupação de utilizar protocolos de transmissão atuais, como IPv6?
( ) Sim
( ) Não
( ) Não sei responder

54. Existe alguma redundância de sistemas de informação, como forma de manter os sistemas operantes na ocorrência de uma falha, garantindo a disponibilidade dos sistemas e dos dados?
( ) Sim
( ) Não
( ) Não sei responder

55. Existe alguma redundância de sistemas de informação, como forma de manter os sistemas operantes na ocorrência de uma falha, garantindo a disponibilidade dos sistemas e dos dados?
( ) Sim
( ) Não
( ) Não sei responder

56. Existe um plano de continuidade documentado na empresa?
( ) Sim
( ) Não
( ) Não sei responder

57. O plano de continuidade, se existente, foi testado?
( ) Sim
( ) Não
( ) Não sei responder

58. Os planos de continuidade garantem que os dados vitais à empresa estejam disponíveis no tempo necessário, conforme os objetivos e estratégias estipulados?
( ) Sim
( ) Não
( ) Não sei responder

APÊNDICE B – QUESTIONÁRIO PARA AVALIAÇÃO FINAL DAS PROPOSTAS DE MELHORIA

As perguntas que seguem têm o objetivo de avaliar a percepção quanto as medidas propostas na realização do Trabalho de Conclusão de Curso de Sistemas de Informação, após a apreciação da proposta encaminhada a cada uma das organização alvo de pesquisa.

1. Como a empresa vê, atualmente, a necessidade de manter dados pessoais em segurança, conforme requisitos da Lei 13.709?

   _____

   _____

2. Foram planejadas ou implementadas ações para se adequar aos requisitos da Lei 13.709? Se sim, quais?

   _____

   _____

3. As medidas apresentadas foram apreciadas pela alta direção da empresa, com o intuito de implementação total ou parcial, em algum momento?

   _____

   _____

4. Dentre as propostas de melhoria apresentada, qual a probabilidade de implementação das mesmas? E qual o prazo previsto para isto, visto que o prazo para a Lei entrar em vigor é fevereiro de 2020?

   _____

   _____

5. Existe, dentre as medidas propostas, alguma que não seja considerada importante para implementação? Por qual motivo?

_____

_____

6. Existe alguma sugestão de alteração nas medidas propostas? Se sim, qual é a sugestão e por qual motivo?

_____

_____

7. Caso exista a intenção de implementar as medidas propostas, parcial ou totalmente, qual a urgência verificada para tomada de ações?

_____

_____

8. A empresa tem consciência que os dados pessoais passam a ter importância equivalente às informações consideradas vitais para a continuidade das operações da mesma?

_____

_____

9. A empresa dispões dos recursos necessários para implementação mínima das melhorias propostas, considerando a data que entra em vigor a Lei (fevereiro de 2020)?

_____

_____

10. Se a implementação das melhorias propostas não for considerada para implementação atualmente, existe a intenção de fazê-lo posteriormente? É possível definir quando?

_____

_____

11. De forma geral, qual a avaliação da proposta do trabalho realizado e das melhorias em segurança da informação propostas, em relação ao atendimento

dos requisitos da Lei 13.709 no que diz respeito a medidas e ferramentas de segurança da informação?

_____

_____

APÊNDICE C – SUGESTÃO DE MELHORIA – EMPRESA ALFA

Proposta de melhoria em segurança da informação direcionado a proteção de dados pessoais

À

Área de Tecnologia da Informação

O presente relatório reúne sugestões de melhorias resultantes da análise realizada quanto às medidas de segurança da informação necessárias para que a empresa se adeque para garantir a proteção de dados pessoais conforme requisitos da Lei 13.709/18. O mesmo faz parte do Trabalho de Conclusão de Curso do aluno Rafael Molin.

Convém que a organização implemente uma Política de Segurança da Informação (PSI), com o objetivo de prover orientação e apoio da direção para manter a segurança da informação e dos dados em acordo com os objetivos e requisitos do negócio, leis e regulamentações relevantes.

A PSI é formada por vários documentos. O primeiro documento contém a diretriz principal, onde são descritos os ativos de informação da empresa, o que é segurança da informação, os princípios que orientam as atividades relativas à segurança da informação, atribuição de responsabilidades para manter a segurança da informação e exceções dos procedimentos de segurança da informação. Esse documento deve ser construído para ter um tempo de vida longo e deve ser assinado pela direção da empresa.

Além do documento de diretriz principal, a PSI é formada por um conjunto de normas de dimensão, que são os métodos e procedimentos para garantir que a utilização dos ativos de informação ocorra de forma segura e somente por pessoal autorizado. As normas de dimensão devem ser construídas em documentos separados, de acordo com os controles necessários a empresa, refletindo as soluções

pretendidas para sanar os riscos de segurança de informação da empresa. Esses documentos devem ser constantemente analisados, revisados e atualizados, de acordo com as alterações de ameaças que a empresa sofre. Para isso é importante que seja realizado uma análise de riscos com uma determinada periodicidade ou quando um incidente de segurança ocorre.

O documento de diretriz principal deve ser de conhecimento de todos funcionários e usuários, além dos agentes externos que tenham acesso a algum sistema ou base de informação da empresa, como representantes ou fornecedores. As normas de dimensão, ao contrário do documento de diretriz principal, deve ser de conhecimento das pessoas afetas a cada uma das normas de dimensão.

É aconselhável, então, que seja implantado um processo de gestão de risco que será utilizado para formular as normas de dimensão da PSI, entre elas: política de controle e acessos, política de segurança física e do ambiente, política de segurança nas operações, política de continuidade dos negócios e políticas e normas de ordem geral.

1. Implantação de um processo de gerenciamento de riscos

Este processo estabelece que a organização conheça e trate os riscos de segurança da informação, devendo existir um procedimento que padronize as ações tomadas para tal. O conhecimento e análise dos riscos iminentes à informação da empresa garante que se adote medidas coesas para que não ocorram incidentes ou, se ocorrerem, os prejuízos sejam conhecidos e controláveis.

Esse procedimento deve apresentar os métodos para:

a) identificar ativos da informação da empresa (lógicos e físicos);

b) as ameaças que podem atingir estes ativos;

c) as vulnerabilidades que podem ser exploradas;

d) os controles já adotados para manter a segurança da informação.

A partir desses, a política deve apresentar as maneiras para identificar os riscos, analisá-los e, assim, definir métodos para reduzir, eliminar, mitigar ou aceitar os riscos identificados. Esses procedimentos devem ser regularmente revisados e

documentados, e todos envolvidos devem estar cientes de seus papéis para manter atualizadas as atividades pertinentes.

O conhecimento e análise dos riscos iminentes à informação da empresa garante que se adote medidas coesas para que não ocorram incidentes ou, se ocorrerem, os prejuízos sejam conhecidos e controláveis. Deve-se atentar para os dados de forma física, que circulam constantemente pela empresa, com quantidade considerável de dados pessoais.

2. Política de Controle de Acesso

Esta documentação estabelece as normas e regras para prover os limites necessários ao acesso à informação e recursos de TI, conforme as reais necessidades de cada usuário. A política deve conter procedimentos documentados para:

a) Gerenciamento de acesso do usuário: procedimentos para registro e cancelamento do acesso aos usuários, gerenciamento dos privilégios de acesso, ajustes dos direitos de acesso, análise crítica dos direitos de acesso e responsabilidades por autorizar / cancelar os acessos, analisar os privilégios e revisar a política regularmente;

b) Controle do acesso do usuário: métodos de autenticação utilizados para acesso do usuário, métodos para controle dos privilégios, métodos para gerenciamento de senhas e procedimentos de análise crítica regularmente executada.

Os usuários devem estar cientes de seus limites quanto aos acessos permitidos, bem como de sua responsabilidade sobre os dados e informações aos quais têm acesso. Convém que a empresa utilize termos de responsabilidade, devidamente assinados pelos usuários quanto aos direitos e deveres no acesso a sistemas de informações e dados, informando as cabíveis penalizações caso irregularidades ou acesso / utilização indevida da informação sejam identificados.

3. Política de segurança física e do ambiente

Este documento configura um conjunto de normas e procedimentos que visa prevenir o acesso físico não autorizado a recursos de processamento da informação e informações da empresa, bem como áreas consideradas críticas pela presença de dados ou informações sensíveis à organização ou dados pessoais.

Devem ser definidos perímetros de segurança, protegendo os ativos e recursos de informação que estejam ali inseridos, como instalações de processamento da informação e áreas que contenham informações críticas ou sensíveis. Departamentos que realizam coleta ou tratamento de dados pessoais devem ser considerados críticos por essa política, bem como as áreas de armazenamento de documentos físicos que contenham dados pessoais do público atendido.

A política de segurança física e do ambiente deve conter:

a) Definição das áreas consideradas de segurança;

b) Métodos de controlar o acesso as áreas de segurança;

c) Definição de pessoal autorizado a acessar as áreas de segurança;

d) Medidas adotadas para manter a segurança das áreas consideradas críticas (construção, trancas de segurança, câmeras de vigilância, registros de acesso, cofres);

e) Métodos de registros de acesso a áreas de segurança;

f) Métodos de controle de circulação de pessoal a áreas de segurança;

g) Métodos de identificação das áreas de segurança e divulgação da importância do controle dessas áreas para todas as pessoas envolvidas.

Convém, também, que a empresa mantenha registro das atividades e procedimentos adotados para controlar a circulação das pessoas em dependências da empresa, bem como as formas de permitir ou não o acesso de pessoal aos departamentos da empresa, de forma geral. Devem ser incluídos nesses controles, o acesso a pessoal externo, como fornecedores, visitantes e público atendido pela empresa, quando cabível.

4. Política de contratação de serviços de informação

Conjunto de procedimentos e normas para contratação de serviços de TI, uma vez que os mesmos não são diretamente prestados pelo pessoal interno a organização. Essa política deve prover métodos para avaliar os seguintes pontos:

a) Definir os requisitos de segurança da informação aplicáveis na aquisição de serviços ou produtos de TI;

b) Definir métodos de monitoramento dos trabalhos executados por terceiros dentro da organização, principalmente quanto existir possibilidade de acesso aos dados e informações da empresa;

c) Definir métodos para permissão de acesso aos sistemas de informação, quando necessário, e os limites de acesso permitidos;

d) Definir meios para responsabilização dos prestadores de serviço quando a manter a segurança nos sistemas de informação e no acesso aos dados e informações existentes nos serviços prestados.

A adoção desses procedimentos evita que qualquer pessoa ou empresa possa vir a acessar, indevidamente, dados considerados críticos ou sensíveis para a organização, minimizando o risco de vazamento de dados ou quebra de segurança.

5. Política para proteção e privacidade de dados pessoais

Deve existir a preocupação constante em relação a dados pessoais que estão presentes na organização, principalmente pela quantidade de dados pessoais coletadas e tratadas diariamente nas operações realizadas. Convém que uma política para proteção e privacidade da informação pessoal seja implementada, estando em conformidade com a legislação vigente, principalmente a Lei 13.709. Esta deve conter informações sobre o que são dados pessoais, como preservá-los de acesso e tratamento indevido, a importância de se manter os dados seguros em todas as operações e as responsabilidades cabíveis aos funcionários da empresa, além de possíveis penalidades que venham a ser consideradas pela organização e pela legislação vigente caso ocorra algum incidente de quebra de segurança.

6. Políticas orientadas ao usuário final

Não menos importantes, devem existir políticas e procedimentos adotados para que o usuário saiba sua responsabilidade em manter a informação segura, seja de forma lógica ou física, conforme segue:

a) Política de mesa e tela limpa, estabelecendo meios para que informações e dados não sejam deixados disponíveis desnecessariamente em mesas de trabalho, computadores ou áreas de uso comum;

b) Uso aceitável de ativos de informação: estabelecer regras para uso dos ativos de informação, como computadores, dispositivos móveis, mídias de armazenamento, relatórios e arquivos impressos que contenham informações pertinentes ao negócio e equipamentos individuais que possam acessar ou interferir nos processos de tratamento de informações da organização;

c) Transferência de informações: definir regras para que a transferência de informações ocorra somente quando necessário, conforme autorizações pré estabelecidas e por meios que garantam a segurança da transferência;

d) Restrições de instalação de softwares e sistemas: definir regras e procedimentos que inibam a instalação indevida de softwares por parte dos usuários. Definir as responsabilidades por avaliar e executar a instalação de softwares e sistemas nos dispositivos da organização.

Essas regras devem ser documentadas e divulgadas para que todos os usuários tenham conhecimento e treinamento sobre seu teor. É aconselhável que se adotem termos de responsabilidade assinados pelos usuários quando cientes de sua responsabilidade referentes a esses procedimentos, bem como possíveis penalizações no caso de ocorrer algum incidente por não seguirem os regramentos definidos.

7. Considerações finais

É importante que, após a implementação das medidas descritas nesse documento, exista o treinamento de todos os envolvidos e usuários, transparecendo as responsabilidades da empresa e de seus funcionários em manter não só os dados da empresa em segurança, como também dados pessoais em seu poder. Os funcionários devem ter conhecimento da importância que as suas atividades têm sobre esses dados, e as consequências que um vazamento ou quebra de segurança de informações críticas ou sensíveis pode ter sobre as operações da empresa.

A implementação das políticas de segurança descritas nesse documento proporciona que existam procedimentos definidos para manter os dados em segurança e, se houver algum incidente que possa prejudicar os sistemas de informação e a continuidade dos negócios, se conheçam as ações que devem ser tomadas e quem deve tomar essas ações. Isso ajuda a reduzir os prejuízos

consequentes de um incidente de segurança, bem como reduz o tempo de tomada de ação para conter os problemas e recuperar os sistemas afetados, de forma organizada e eficaz, desde que os planos para tal estejam bem definidos e implementados.

Para auxiliar na implementação das políticas, aconselha-se a utilização das Normas ABNT da série ISO/IEC 27000, as quais apresentam práticas para controle de segurança da informação de forma bem abrangente, para qualquer tipo de organização.

APÊNDICE D – SUGESTÃO DE MELHORIA – EMPRESA BETA

Proposta de melhoria em segurança da informação direcionado a proteção de dados pessoais

À

Área de Tecnologia da Informação

O presente relatório reúne sugestões de melhorias resultantes da análise realizada quanto às medidas de segurança da informação necessárias para que a empresa se adeque para garantir a proteção de dados pessoais conforme requisitos da Lei 13.709/18. O mesmo faz parte do Trabalho de Conclusão de Curso do aluno Rafael Molin.

Convém que a organização implemente uma Política de Segurança da Informação (PSI), com o objetivo de prover orientação e apoio da direção para manter a segurança da informação e dos dados em acordo com os objetivos e requisitos do negócio, leis e regulamentações relevantes.

A PSI é formada por vários documentos. O primeiro documento contém a diretriz principal, onde são descritos os ativos de informação da empresa, o que é segurança da informação, os princípios que orientam as atividades relativas à segurança da informação, atribuição de responsabilidades para manter a segurança da informação e exceções dos procedimentos de segurança da informação. Esse documento deve ser construído para ter um tempo de vida longo e deve ser assinado pela direção da empresa.

Além do documento de diretriz principal, a PSI é formada por um conjunto de normas de dimensão, que são os métodos e procedimentos para garantir que a utilização dos ativos de informação ocorra de forma segura e somente por pessoal autorizado. As normas de dimensão devem ser construídas em documentos separados, de acordo com os controles necessários a empresa, refletindo as soluções

pretendidas para sanar os riscos de segurança de informação da empresa. Esses documentos devem ser constantemente analisados, revisados e atualizados, de acordo com as alterações de ameaças que a empresa sofre. Para isso é importante que seja realizado uma análise de riscos com uma determinada periodicidade ou quando um incidente de segurança ocorre.

O documento de diretriz principal deve ser de conhecimento de todos funcionários e usuários, além dos agentes externos que tenham acesso a algum sistema ou base de informação da empresa, como representantes ou fornecedores. As normas de dimensão, ao contrário do documento de diretriz principal, deve ser de conhecimento das pessoas afetas a cada uma das normas de dimensão.

É aconselhável, então, que seja implantado um processo de gestão de risco que será utilizado para formular as normas de dimensão da PSI, entre elas: política de controle e acessos, política de segurança física e do ambiente, política de segurança nas operações, política de continuidade dos negócios e políticas e normas de ordem geral.

1. Implantação de um processo de análise de riscos

Este processo estabelece que a organização conheça e trate os riscos de segurança da informação, devendo existir um procedimento que padronize as ações tomadas para tal. O conhecimento e análise dos riscos iminentes à informação da empresa garante que se adote medidas coesas para que não ocorram incidentes ou, se ocorrerem, os prejuízos sejam conhecidos e controláveis.

Esse procedimento deve apresentar os métodos para:

a) identificar ativos da informação da empresa (lógicos e físicos);

b) as ameaças que podem atingir estes ativos;

c) as vulnerabilidades que podem ser exploradas;

d) os controles já adotados para manter a segurança da informação.

A partir desses, o processo de análise deve apresentar as maneiras para identificar os riscos, analisá-los e, assim, definir métodos para reduzir, eliminar, mitigar

ou aceitar os riscos identificados. Esses procedimentos devem ser regularmente revisados e documentados, e todos envolvidos devem estar cientes de seus papéis para manter atualizadas as atividades pertinentes.

2. Política de Controle de Acesso

Esta documentação estabelece as normas e regras para prover os limites necessários ao acesso à informação e recursos de TI, conforme as reais necessidades de cada usuário. A política deve conter procedimentos documentados para:

a) Gerenciamento de acesso do usuário: procedimentos para registro e exclusão do acesso aos usuários, gerenciamento dos privilégios de acesso a cada usuário ou grupo de usuários, ajustes dos direitos de acesso, análise crítica dos direitos de acesso e responsabilidades por autorizar / cancelar os acessos, analise dos privilégios de acesso e revisão periódica da política;

b) Controle do acesso do usuário: métodos de autenticação utilizados para acesso do usuário, métodos para controle dos privilégios, métodos para gerenciamento de senhas e procedimentos de análise crítica regularmente executada.

Os usuários devem estar cientes de seus limites quanto aos acessos permitidos, bem como de sua responsabilidade sobre os dados e informações aos quais têm acesso. Convém que a empresa utilize termos de responsabilidade, devidamente assinados pelos usuários quanto aos direitos e deveres no acesso a sistemas de informações e dados, informando as cabíveis penalizações caso irregularidades ou acesso / utilização indevida da informação sejam identificados.

3. Política de segurança física e do ambiente

Este documento configura um conjunto de normas e procedimentos que visa prevenir o acesso físico não autorizado a recursos de processamento da informação e informações da empresa, bem como áreas consideradas críticas pela presença de dados ou informações sensíveis à organização ou dados pessoais.

É extremamente aconselhável que exista a definição dos perímetros de segurança, protegendo os ativos e recursos de informação que estejam ali inseridos, como instalações TI e áreas que contenham informações críticas ou sensíveis à organização (incluindo dados pessoais).

A política de segurança física e do ambiente deve conter:

a) Definição das áreas consideradas de segurança;

b) Métodos de controlar o acesso as áreas de segurança;

c) Definição de pessoal autorizado a acessar as áreas de segurança;

d) Medidas adotadas para manter a segurança das áreas consideradas críticas (construção, trancas de segurança, câmeras de vigilância, registros de acesso, cofres ou armários com trancas);

e) Métodos de registros de acesso a áreas de segurança;

f) Métodos de controle de circulação de pessoal em áreas de segurança;

g) Métodos de identificação das áreas de segurança e divulgação da importância do controle dessas áreas para todas as pessoas envolvidas.

Convém, também, que a empresa mantenha registro das atividades e procedimentos adotados para controlar a circulação das pessoas em dependências da empresa, bem como as formas de permitir ou não o acesso de pessoal aos departamentos da empresa, de forma geral, procurando manter o controle de que somente pessoal autorizado tenha acesso aos dados da organização e dados pessoais. Devem ser incluídos nesses controles, o acesso a pessoal externo, como fornecedores, visitantes e clientes da empresa.

4. Política de Segurança nas Operações

Conjunto de normas e procedimentos para definir os métodos seguros de operação dos recursos de processamento da informação. Devem estar documentados os procedimentos considerados seguros e padronizados para:

a) Instalação e configuração de sistemas, softwares e equipamentos de TI;

b) Processamento e tratamento de dados e informação (tanto automática como manual);

c) Implantação de componentes de segurança e sua configuração (firewall, proxy, detecção de invasão de rede, antivírus e similares);

d) Requisitos de agendamento de tarefas automatizadas em sistemas de informação;

e) Análise de capacidade e disponibilidade dos sistemas de informação;

f) Procedimentos de monitoramento das operações.

Os procedimentos adotados e documentados devem ser de conhecimento de todos os usuários que necessitam deles, proporcionando que as operações não sejam prejudicadas por falta de responsabilizações pelas tarefas descritas nos procedimentos ou pelo não conhecimento por parte dos usuários de suas responsabilidades e deveres em manter os sistemas operantes e em segurança.

Também deve existir meios documentados para revisão periódica dos procedimentos adotados, garantindo que estes sejam atuais e coerentes com os objetivos observados na PSI.

5. Política de Continuidade dos Negócios

A empresa deve possuir uma política definida e implementada para garantir que as operações dos sistemas de informação mantenham-se operantes conforme as necessidades do negócio, mesmo após a ocorrência de incidentes que possam as prejudicar de alguma maneira (os riscos devem ser conhecidos e analisados conforme a análise de riscos comentada anteriormente nesse documento).

Quanto ao gerenciamento de cópias de segurança, deve haver procedimentos para:

a) Informar as rotinas implementadas para geração das cópias de segurança (backups);

b) Definir quais as mídias e meios para armazenar os dados;

c) Definir quais os dados e informações devem ser mantidos em cópias de segurança e por quanto tempo devem ser guardados esses dados;

d) Definir os métodos para testar periodicamente a integridade das mídias e do processo de recuperação de dados;

e) Definir os responsáveis pelas ações que devem ser tomadas, tanto para geração das cópias de segurança, quanto para recuperação de dados, quando necessário;

f) Analisar criticamente e periodicamente os procedimentos adotados para manter cópias de segurança dos dados e informações da empresa.

Quanto a continuidade das operações, devem existir procedimentos para:

a) Definir os métodos de redundância de sistemas adotados para manter os sistemas operantes;

b) Definir como os métodos de redundância são configurados para entrar em operação, caso ocorra um incidente;

c) Definir métodos de testar e analisar os sistemas de redundância adotados;

d) Definir as responsabilidades necessárias na ocorrência de uma falha ou incidente, procurando reduzir os impactos às operações da organização;

e) Definir métodos de análise periódica dos métodos adotados para verificar sua eficácia conforme as necessidades de negócio da empresa.

Todos os envolvidos nos processos de continuidade de negócio devem conhecer os procedimentos adotados nessa política, entendendo a responsabilidade em manter os serviços de informação operantes conforme as necessidades do negócio e a segurança dos dados e informações.

6. Políticas e normas de ordem geral

Não menos importantes, devem existir políticas e procedimentos adotados para que o usuário saiba sua responsabilidade em manter a informação segura, seja de forma lógica ou física, conforme segue:

a) Política de mesa e tela limpa, estabelecendo meios para que informações e dados não sejam deixados disponíveis desnecessariamente em mesas de trabalho, computadores ou áreas de uso comum;

b) Uso aceitável de equipamentos de TI e ativos de informação: estabelecer regras para uso dos ativos de informação, como computadores, dispositivos móveis, mídias de armazenamento, impressoras, relatórios e arquivos impressos que

contenham informações pertinentes ao negócio e equipamentos individuais que possam acessar ou interferir nos processos de tratamento de informações da organização;

c) Transferência de informações: definir regras para que a transferência de informações ocorra somente quando necessário, conforme autorizações preestabelecidas e por meios que garantam a segurança da transferência;

d) Restrições de instalação de softwares e sistemas: definir regras e procedimentos que inibam a instalação indevida de softwares por parte dos usuários. Definir as responsabilidades por avaliar e executar a instalação de softwares e sistemas nos dispositivos da organização.

Essas regras devem ser documentadas e divulgadas para que todos os usuários tenham conhecimento e treinamento sobre seu teor. É aconselhável que se adotem termos de responsabilidade assinados pelos usuários quando cientes de sua responsabilidade referentes a esses procedimentos, bem como possíveis penalizações no caso de ocorrer algum incidente por não seguirem os regramentos definidos.

7. Considerações finais

É importante que, após a implementação das medidas descritas nesse documento, exista o treinamento de todos os envolvidos e usuários, transparecendo as responsabilidades da empresa e de seus funcionários em manter não só os dados da empresa em segurança, como também dados pessoais em seu poder. Os funcionários devem ter conhecimento da importância que as suas atividades têm sobre esses dados, e as consequências que um vazamento ou quebra de segurança de informações críticas ou sensíveis pode ter sobre as operações da empresa.

A implementação das políticas de segurança descritas nesse documento proporciona que existam procedimentos definidos para manter os dados em segurança e, se houver algum incidente que possa prejudicar os sistemas de informação e a continuidade dos negócios, se conheçam as ações que devem ser tomadas e quem deve tomar essas ações. Isso ajuda a reduzir os prejuízos consequentes de um incidente de segurança, bem como reduz o tempo de tomada de

ação para conter os problemas e recuperar os sistemas afetados, de forma organizada e eficaz, desde que os planos para tal estejam bem definidos e implementados.

Para auxiliar na implementação das políticas, aconselha-se a utilização das Normas ABNT da série ISO/IEC 27000, as quais apresentam práticas para controle de segurança da informação de forma bem abrangente, para qualquer tipo de organização.

APÊNDICE E – SUGESTÃO DE MELHORIA – EMPRESA GAMA

Proposta de melhoria em segurança da informação direcionado a proteção de dados pessoais

À

Área de Tecnologia da Informação

O presente relatório reúne sugestões de melhorias resultantes da análise realizada quanto às medidas de segurança da informação necessárias para que a empresa se adeque para garantir a proteção de dados pessoais conforme requisitos da Lei 13.709/18. O mesmo faz parte do Trabalho de Conclusão de Curso do aluno Rafael Molin.

Convém que a organização implemente uma Política de Segurança da Informação (PSI), com o objetivo de prover orientação e apoio da direção para manter a segurança da informação e dos dados em acordo com os objetivos e requisitos do negócio, leis e regulamentações relevantes.

A PSI é formada por vários documentos. O primeiro documento contém a diretriz principal, onde são descritos os ativos de informação da empresa, o que é segurança da informação, os princípios que orientam as atividades relativas à segurança da informação, atribuição de responsabilidades para manter a segurança da informação e exceções dos procedimentos de segurança da informação. Esse documento deve ser construído para ter um tempo de vida longo e deve ser assinado pela direção da empresa.

Além do documento de diretriz principal, a PSI é formada por um conjunto de normas de dimensão, que são os métodos e procedimentos para garantir que a utilização dos ativos de informação ocorra de forma segura e somente por pessoal autorizado. As normas de dimensão devem ser construídas em documentos separados, de acordo com os controles necessários a empresa, refletindo as soluções

pretendidas para sanar os riscos de segurança de informação da empresa. Esses documentos devem ser constantemente analisados, revisados e atualizados, de acordo com as alterações de ameaças que a empresa sofre. Para isso é importante que seja realizado uma análise de riscos com uma determinada periodicidade ou quando um incidente de segurança ocorre.

O documento de diretriz principal deve ser de conhecimento de todos funcionários e usuários, além dos agentes externos que tenham acesso a algum sistema ou base de informação da empresa, como representantes ou fornecedores. As normas de dimensão, ao contrário do documento de diretriz principal, deve ser de conhecimento das pessoas afetas a cada uma das normas de dimensão.

É aconselhável, então, que seja implantado um processo de gestão de risco que será utilizado para formular as normas de dimensão da PSI, entre elas: política de controle e acessos, política de segurança física e do ambiente, política de segurança nas operações, política de continuidade dos negócios e políticas e normas de ordem geral.

1. Implantação de um processo de análise de riscos

Este processo estabelece que a organização conheça e trate os riscos de segurança da informação, devendo existir um procedimento que padronize as ações tomadas para tal. O conhecimento e análise dos riscos iminentes à informação da empresa garante que se adote medidas coesas para que não ocorram incidentes ou, se ocorrerem, os prejuízos sejam conhecidos e controláveis.

Esse procedimento deve apresentar os métodos para:

a) identificar ativos da informação da empresa (lógicos e físicos);

b) as ameaças que podem atingir estes ativos;

c) as vulnerabilidades que podem ser exploradas;

d) os controles já adotados para manter a segurança da informação.

A partir desses, o processo de análise deve apresentar as maneiras para identificar os riscos, analisá-los e, assim, definir métodos para reduzir, eliminar, mitigar

ou aceitar os riscos identificados. Esses procedimentos devem ser regularmente revisados e documentados, e todos envolvidos devem estar cientes de seus papéis para manter atualizadas as atividades pertinentes.

2. Política de Controle de Acesso

Esta documentação estabelece as normas e regras para prover os limites necessários ao acesso à informação e recursos de TI, conforme as reais necessidades de cada usuário. A política deve conter procedimentos documentados para:

a) Gerenciamento de acesso do usuário: procedimentos para registro e exclusão do acesso aos usuários, gerenciamento dos privilégios de acesso a cada usuário ou grupo de usuários, ajustes dos direitos de acesso, análise crítica dos direitos de acesso e responsabilidades por autorizar / cancelar os acessos, analise dos privilégios de acesso e revisão periódica da política;

b) Controle do acesso do usuário: métodos de autenticação utilizados para acesso do usuário, métodos para controle dos privilégios, métodos para gerenciamento de senhas e procedimentos de análise crítica regularmente executada.

Os usuários devem estar cientes de seus limites quanto aos acessos permitidos, bem como de sua responsabilidade sobre os dados e informações aos quais têm acesso. Convém que a empresa utilize termos de responsabilidade, devidamente assinados pelos usuários quanto aos direitos e deveres no acesso a sistemas de informações e dados, informando as cabíveis penalizações caso irregularidades ou acesso / utilização indevida da informação sejam identificados.

3. Política de segurança física e do ambiente

Este documento configura um conjunto de normas e procedimentos que visa prevenir o acesso físico não autorizado a recursos de processamento da informação e informações da empresa, bem como áreas consideradas críticas pela presença de dados ou informações sensíveis à organização ou dados pessoais.

É extremamente aconselhável que exista a definição dos perímetros de segurança, protegendo os ativos e recursos de informação que estejam ali inseridos, como instalações TI e áreas que contenham informações críticas ou sensíveis à organização (incluindo dados pessoais).

A política de segurança física e do ambiente deve conter:

a) Definição das áreas consideradas de segurança;

b) Métodos de controlar o acesso as áreas de segurança;

c) Definição de pessoal autorizado a acessar as áreas de segurança;

d) Medidas adotadas para manter a segurança das áreas consideradas críticas (construção, trancas de segurança, câmeras de vigilância, registros de acesso, cofres ou armários com trancas);

e) Métodos de registros de acesso a áreas de segurança;

f) Métodos de controle de circulação de pessoal em áreas de segurança;

g) Métodos de identificação das áreas de segurança e divulgação da importância do controle dessas áreas para todas as pessoas envolvidas.

Convém, também, que a empresa mantenha registro das atividades e procedimentos adotados para controlar a circulação das pessoas em dependências da empresa, bem como as formas de permitir ou não o acesso de pessoal aos departamentos da empresa, de forma geral, procurando manter o controle de que somente pessoal autorizado tenha acesso aos dados da organização e dados pessoais. Devem ser incluídos nesses controles, o acesso a pessoal externo, como fornecedores, visitantes e clientes da empresa.

4. Política de Segurança nas Operações

Conjunto de normas e procedimentos para definir os métodos seguros de operação dos recursos de processamento da informação. Devem estar documentados os procedimentos considerados seguros e padronizados para:

a) Instalação e configuração de sistemas, softwares e equipamentos de TI;

b) Processamento e tratamento de dados e informação (tanto automática como manual);

c) Implantação de componentes de segurança e sua configuração (firewall, proxy, detecção de invasão de rede, antivírus e similares);

d) Requisitos de agendamento de tarefas automatizadas em sistemas de informação;

e) Análise de capacidade e disponibilidade dos sistemas de informação;

f) Procedimentos de monitoramento das operações.

Os procedimentos adotados e documentados devem ser de conhecimento de todos os usuários que necessitam deles, proporcionando que as operações não sejam prejudicadas por falta de responsabilizações pelas tarefas descritas nos procedimentos ou pelo não conhecimento por parte dos usuários de suas responsabilidades e deveres em manter os sistemas operantes e em segurança.

Também deve existir meios documentados para revisão periódica dos procedimentos adotados, garantindo que estes sejam atuais e coerentes com os objetivos observados na PSI.

5. Política de Continuidade dos Negócios

A empresa deve possuir uma política definida e implementada para garantir que as operações dos sistemas de informação mantenham-se operantes conforme as necessidades do negócio, mesmo após a ocorrência de incidentes que possam as prejudicar de alguma maneira (os riscos devem ser conhecidos e analisados conforme a análise de riscos comentada anteriormente nesse documento).

Quanto ao gerenciamento de cópias de segurança, deve haver procedimentos para:

a) Informar as rotinas implementadas para geração das cópias de segurança (backups);

b) Definir quais as mídias e meios para armazenar os dados;

c) Definir quais os dados e informações devem ser mantidos em cópias de segurança e por quanto tempo devem ser guardados esses dados;

d) Definir os métodos para testar periodicamente a integridade das mídias e do processo de recuperação de dados;

e) Definir os responsáveis pelas ações que devem ser tomadas, tanto para geração das cópias de segurança, quanto para recuperação de dados, quando necessário;

f) Analisar criticamente e periodicamente os procedimentos adotados para manter cópias de segurança dos dados e informações da empresa.

Quanto a continuidade das operações, devem existir procedimentos para:

a) Definir os métodos de redundância de sistemas adotados para manter os sistemas operantes;

b) Definir como os métodos de redundância são configurados para entrar em operação, caso ocorra um incidente;

c) Definir métodos de testar e analisar os sistemas de redundância adotados;

d) Definir as responsabilidades necessárias na ocorrência de uma falha ou incidente, procurando reduzir os impactos às operações da organização;

e) Definir métodos de análise periódica dos métodos adotados para verificar sua eficácia conforme as necessidades de negócio da empresa.

Todos os envolvidos nos processos de continuidade de negócio devem conhecer os procedimentos adotados nessa política, entendendo a responsabilidade em manter os serviços de informação operantes conforme as necessidades do negócio e a segurança dos dados e informações.

6. Políticas e normas de ordem geral

Não menos importantes, devem existir políticas e procedimentos adotados para que o usuário saiba sua responsabilidade em manter a informação segura, seja de forma lógica ou física, conforme segue:

a) Política de mesa e tela limpa, estabelecendo meios para que informações e dados não sejam deixados disponíveis desnecessariamente em mesas de trabalho, computadores ou áreas de uso comum;

b) Uso aceitável de equipamentos de TI e ativos de informação: estabelecer regras para uso dos ativos de informação, como computadores, dispositivos móveis, mídias de armazenamento, impressoras, relatórios e arquivos impressos que contenham informações pertinentes ao negócio e equipamentos individuais que possam acessar ou interferir nos processos de tratamento de informações da organização;

c) Transferência de informações: definir regras para que a transferência de informações ocorra somente quando necessário, conforme autorizações preestabelecidas e por meios que garantam a segurança da transferência;

d) Restrições de instalação de softwares e sistemas: definir regras e procedimentos que inibam a instalação indevida de softwares por parte dos usuários. Definir as responsabilidades por avaliar e executar a instalação de softwares e sistemas nos dispositivos da organização.

Essas regras devem ser documentadas e divulgadas para que todos os usuários tenham conhecimento e treinamento sobre seu teor. É aconselhável que se adotem termos de responsabilidade assinados pelos usuários quando cientes de sua responsabilidade referentes a esses procedimentos, bem como possíveis penalizações no caso de ocorrer algum incidente por não seguirem os regramentos definidos.

7. Considerações finais

É importante que, após a implementação das medidas descritas nesse documento, exista o treinamento de todos os envolvidos e usuários, transparecendo as responsabilidades da empresa e de seus funcionários em manter não só os dados da empresa em segurança, como também dados pessoais em seu poder. Os funcionários devem ter conhecimento da importância que as suas atividades têm sobre esses dados, e as consequências que um vazamento ou quebra de segurança de informações críticas ou sensíveis pode ter sobre as operações da empresa.

A implementação das políticas de segurança descritas nesse documento proporciona que existam procedimentos definidos para manter os dados em segurança e, se houver algum incidente que possa prejudicar os sistemas de informação e a continuidade dos negócios, se conheçam as ações que devem ser tomadas e quem deve tomar essas ações. Isso ajuda a reduzir os prejuízos consequentes de um incidente de segurança, bem como reduz o tempo de tomada de ação para conter os problemas e recuperar os sistemas afetados, de forma organizada e eficaz, desde que os planos para tal estejam bem definidos e implementados.

Para auxiliar na implementação das políticas, aconselha-se a utilização das Normas ABNT da série ISO/IEC 27000, as quais apresentam práticas para controle

de segurança da informação de forma bem abrangente, para qualquer tipo de organização.