ISSN 1808-6136
ISSN on-line 2674-7499

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UMA PROPOSTA APLICADA AO CONTEXTO DA LGPD

NILTON FREITAS JUNIOR[1]; ALYSON SILVA FERREIRA[2]

[1] Mestre em Pesquisa Operacional e Inteligência Computacional pela Universidade Cândido Mendes. Professor do Centro Universitário UniFaminas, Muriaé. Professor e Chefe do Departamento de Ciências Exatas da Universidade do Estado de Minas Gerais, Carangola. E-mail: niltonfjunior@gmail.com.
[2] Bacharel em Sistemas de Informação pela Universidade do Estado de Minas Gerais – Unidade Carangola. E-mail: alysonsilva99@hotmail.com.

RESUMO
Este trabalho apresenta um estudo baseado na Lei 13.709/18, também conhecida como Lei Geral de Proteção de Dados (LGPD), criada para fornecer a segurança de dados pessoais sensíveis, monitorando as formas de tratamento adotadas pelas organizações, aplicando sanções correspondentes ao seu descumprimento e incentivando a adoção de Normas Técnicas que facilitem o controle dos dados por seus titulares. Diante disso, o objetivo central deste estudo foi o desenvolvimento de um Modelo de Política de Segurança da Informação, capaz de atender os princípios impostos pela lei. Para essa ação foram realizadas pesquisas de cunho qualitativo em meios *online*, como *sites*, artigos, livros e o próprio texto-base da lei. Com as informações obtidas juntamente à utilização de ferramentas comuns a maioria das pessoas (Word e Excel), obteve-se exemplos de Modelos Adaptáveis de uma 'PSI' e um 'Termo de Responsabilidade', que podem vir a ser utilizados por empresas que busquem se adaptar a LGPD.
Palavras-chave: LGPD; Política de Segurança da Informação; Proteção de Dados Pessoais.

INFORMATION SECURITY POLICY: A PROPOSAL APPLIED TO THE CONTEXT OF THE LGPD

ABSTRACT
This paper presents a study based on Law 13.709/18, also known as the General Data Protection Law (LGPD), created to provide security for sensitive personal data by monitoring the treatment methods adopted by organizations, applying sanctions corresponding to non-compliance, and encouraging the adoption of Technical Standards that facilitate data control by their holders. Therefore, the main objective of this study was the development of an Information Security Policy Model capable of meeting the principles imposed by the law. For this purpose, qualitative research was conducted through online means such as websites, articles, books, and the law's basic text. With the obtained information, along with the use of tools commonly accessible to most people (Word and Excel), examples of Adaptable Models of an 'ISP' and a 'Responsibility Term' were developed, which can be used by companies seeking to adapt to the LGPD.
Keywords: LGPD; Information Security Policy; Personal Data Protection.

1 INTRODUÇÃO

As influências das Tecnologias da Informação (TI) estão cada vez mais presentes na sociedade, proporcionando frequente surgimento de novos produtos e serviços. Muito desse aumento tecnológico se deu com a popularização da *Internet*, responsável por manter novos paradigmas de ambientes de trabalho, estudo, comunicação e lazer, aliando-se a dispositivos cada vez mais interativos e tornando plausível a percepção de que a TI está cada vez mais inserida em vários aspectos do cotidiano das pessoas.

Recebido em 15/08/2024 e aprovado para publicação em 21/01/2025.

Tamanha a abrangência vista com a presença da TI na sociedade leva à necessidade de novas compreensões sobre o tratamento dos dados gerados na utilização dos inúmeros recursos disponíveis para as pessoas. É perceptível um cenário onde o mundo real e o mundo digital já não são universos diferentes, dada a maciça produção de dados seja nas chamadas redes sociais ou mesmo nos diversos sistemas de informação utilizados por organizações dos mais diversos tipos de atuação no mercado.

A transformação de informações em recursos úteis é essencial no contexto das organizações modernas, onde os dados assumem um papel cada vez mais estratégico. Dados separados não apresentam caráter qualitativo, uma vez que se trata de apreensões de fatos que possuem pouca ou nenhuma correlação entre si. Porém, uma vez que a estes dados sejam aplicados processamentos, surge o conceito da informação, que invariavelmente carrega consigo grande valor para processos de tomadas de decisão (DE MATTOS, 2010).

Neste aspecto, a existência de dados produzidos nos ambientes digitais e que possuem características de cunho pessoal destaca-se pela tendência a representar uma ameaça à privacidade dos indivíduos. Considerando isso, para manter a segurança de dados sensíveis torna-se necessário o desenvolvimento de novos paradigmas que sejam capazes de garantir uma maior proteção quanto aos processamentos aplicados a estes dados e ao uso das informações geradas.

A proteção aos dados pessoais já é uma realidade em vários países, que possuem legislações criadas para garantir o uso adequado desses dados, estabelecendo regras para seu tratamento. Recentemente, o Brasil criou uma legislação própria para esta mesma finalidade, tomando como referência os padrões já existentes ao redor do globo. Assim surge a Lei Geral de Proteção de Dados (LGPD), aprovada em agosto de 2018, entrando em vigor no mês de setembro de 2020 (AGÊNCIA SENADO, 2020).

Essa legislação chega para mudar a forma como os dados pessoais são tratados no país, dando maior controle aos titulares detentores desses dados. No que confere a LGPD n. 13.709/2018, estabelece-se em seu artigo 1º que seu objetivo é garantir o tratamento de dados de pessoas naturais ou jurídicas em meios físicos e digitais, visando proteger os direitos fundamentais de liberdade e privacidade de cada indivíduo (BRASIL, 2018).

Segundo Fontes (2012), a Segurança da Informação não se restringe somente a *hardwares* e *softwares*, mas vai muito além da área de TI. O tratamento de dados de forma segura é um tema recorrente dentro das empresas há algum tempo, e o surgimento da LGPD o tornou ainda mais necessário, demandando maior atenção e investimentos no setor.

A construção deste trabalho busca tornar evidente os conceitos de Segurança da Informação em ambientes organizacionais, de forma que exigências impostas pela LGPD sejam atendidas corretamente. Como o conceito de Segurança da Informação está presente em diversos estudos na formação acadêmica de profissionais de Sistemas de Informação, surge a oportunidade de agregar novos conhecimentos aos já existentes, além de garantir a esses profissionais um maior domínio sobre o assunto.

Diante disso, torna-se a necessidade do estabelecimento de uma Política de Segurança da Informação dentro de empresas, dada a importância no tratamento de dados pessoais imposta pela LGPD. Com isso, pode-se estabelecer o seguinte questionamento: é possível apresentar um modelo de documentação sobre posturas de Segurança da Informação, aplicável a empresas que desejam se adequar aos princípios da LGPD?

Este trabalho tem como objetivo geral apresentar um modelo de documentação do tipo Política de Segurança da Informação, com conteúdo adaptável aos princípios da Lei Geral de Proteção de Dados (Lei 13.709/18), visando sua aplicação prática em empresas que buscam se adequar a essa legislação. Para isso, busca-se apresentar conteúdo teórico que ampare a construção da documentação proposta, detalhando os tópicos indispensáveis em uma Política de Segurança da Informação, além de exibir o texto adaptável construído e o processo de elaboração com as ferramentas utilizadas. Com isso, pode-se estabelecer o seguinte questionamento: é possível apresentar um modelo de documentação sobre posturas de Segurança da Informação, aplicável a empresas que desejam se adequar aos princípios da LGPD?

A justificativa para a realização deste estudo fundamenta-se na crescente importância da Segurança da Informação, impulsionada pelas exigências da LGPD, que tornou essencial a criação de políticas que assegurem o tratamento adequado de dados sensíveis, permitindo às organizações atender às exigências legais e garantir a proteção de informações de seus colaboradores e clientes.

2 REFERENCIAL TEÓRICO

2.1 Dados, Processamento e Informação

As definições de Dados, em sua maioria, mostram o emprego da palavra de uma forma mais geral. Mas de todos os conceitos, destaca-se a termologia utilizada pela área da informática. Neste campo de estudo, Ferreira *et al.* (1999, p. 602) afirma que Dado é um "elemento de informação, ou representação de fatos ou instruções, em forma apropriada para

armazenamento, processamento ou transmissão por meios automáticos", que completa o que é dito por Houaiss *et al.* (2001), para quem os dados são todas e quaisquer informações capazes de serem processadas por um computador.

O Processamento de Dados por sua vez é composto por diversas atividades ordenadas e que ocorrem de forma conjunta entre *hardware* e *software*, transformando os dados em informações (MARTINELLI; VENTURA, 2006). Esse processamento tem por objetivo fornecer os resultados necessários aos consumidores finais, convertendo os dados que se encontram de forma bruta em um aglomerado de dados mais significativos que representam informação (LAUDON; JANE, 2004).

As ações realizadas no processamento resultam na Informação, que pode ser compreendida como o ato ou efeito de informar. Já em um contexto científico é defendido que o seu significado seja mais completo, sendo vista como o principal conceito de Sistemas de Informação e um recurso de grande valor para a sociedade atual (AUDY; ANDRADE; CIDRAL, 2005). Informações são os dados que foram organizados ou analisados durante o processamento e que, ao fim do processo, se apresentam de forma adequada à sua finalidade (STONER; FREEMAN, 1999).

2.2 Segurança da Informação

Segurança da Informação é um termo que surgiu conforme o crescimento do fluxo de informações, dentro dos vários sistemas computacionais existentes. A importância da informação nos contextos dos processos de tomada de decisões fez com que esta se tornasse um ativo[1] importante e essencial para as organizações, necessitando de proteção (ABNT NBR ISO/IEC 27002:2005). Surge dessa forma definições do termo por diversos autores. Sêmola (2003, p.43), define a Segurança da Informação como "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade". Em seu trabalho, Bastos e Caubit (2009) oferecem uma definição mais aprofundada para a Segurança da Informação:

> A segurança de informação é caracterizada pela aplicação adequada de dispositivos de proteção sobre um ativo ou um conjunto de ativos visando preservar o valor que este possui para as organizações. A aplicação destas proteções busca preservar a confidencialidade, a integridade e a disponibilidade (CID), não estando restritos somente a sistemas ou aplicativos, mas também informações armazenadas ou veiculadas em diversos meios além do eletrônico ou em papel (BASTOS; CAUBIT, 2009, p. 17).

[1] Um ativo é um bem ou direito necessário para a execução ou manutenção das atividades de uma organização.

Assim, é perceptível que a Segurança da Informação visa à proteção da informação enquanto ativo, de forma adequada, em busca de evitar quaisquer tipos de adversidades. No entanto, a Segurança da Informação sozinha não apresenta valor algum, ela necessita estar alinhada aos objetivos da organização.

Para cumprir os objetivos tem sido comum às organizações aderirem a Políticas de Segurança da Informação (PSI), defendidas por Fontes (2012), que aponta que para a existência de atividade de segurança, é imprescindível a construção de políticas e leis de proteção. Silva, Carvalho e Torres (2003) complementam dizendo que a proteção é necessária para que os impactos causados por ameaças sejam reduzidos. Para atender a essas políticas é necessário o cumprimento de três princípios básicos: Confidencialidade, Integridade e Disponibilidade (CID), considerados os pilares da Segurança da Informação, conforme Lyra (2008, p. 4).

Conforme as informações se tornaram um ativo valioso, a influência exercida pelas mesmas dentro da competitividade de mercado ascenderam. Por isso, aqueles que utilizam de métodos que asseguram a confidencialidade se destacam perante o mercado, sendo o motivo principal a "garantia de que o acesso à informação é restrito aos seus usuários legítimos." (BEAL, 2008, p.1), podendo também ser destacado que a confidencialidade pode assumir duas formas de ação, restringindo o entendimento da informação de forma parcial ou completa (MENEZES *et al.*, 1996).

Todo o valor apresentado por uma informação está na sua fidedignidade, qualquer alteração apresentada, mesmo que mínima, pode comprometer a integridade e causar prejuízos enormes. Para Sêmola (2003), as informações devem ser mantidas em sua condição inicial, com o objetivo de proteção contra qualquer alteração, seja ela: intencional, acidental ou indevida. Para que esses problemas não ocorram, é muito comum que sistemas de qualidade apresentem serviços com características de identificação, permitindo a análise de possíveis alterações ocorridas (WALTERS *et al.*, 2006).

Um problema que pode ser recorrente é a não possibilidade de acesso a alguma informação no exato momento que se necessita dela, o que é algo equivalente a não ter informações. Nesse momento entra em destaque a importância da disponibilidade que deve garantir que os dispositivos forneçam o que se espera deles. Para Zhoue e Fang (2009), esse provavelmente é o serviço mais extensivo, já que abrange quase todos os aspectos dentro de uma rede. Portanto, independente dos fins, uma informação deve estar sempre disponível e a sua ausência pode causar o comprometimento de ações.

2.3 Lei 13.709/18 - Lei Geral de Proteção de Dados Pessoais

Sendo considerados os princípios de Segurança da Informação, pode-se inferir que a existência de uma legislação capaz de proteger os dados pessoais não somente é uma necessidade, como também direito dos cidadãos. Fatos como a conectividade à *internet*, serviços bancários por meio de aplicativos e ferramentas modernas de coleta e processamento de dados começaram a causar preocupações acerca da segurança.

Juntamente ao aumento no uso de serviços em ambientes de sistemas de informação, seja *online* ou não, observou-se também um crescimento de falhas de segurança e vazamentos de dados. Baseando-se nisso, discussões sobre a forma como os dados eram utilizados em todo o mundo se tornaram recorrentes, sendo o principal motivo para que a União Europeia aprovasse a *General Data Protection Regulation* (GDPR), um documento composto por normas e sanções, com o intuito proteger os dados pessoais (CAETANO, 2020)

Com o surgimento da GDPR, a *internet* como um todo foi afetada, impondo a *sites* e empresas que se adequassem às novas regras. Tomando como base as mudanças que essa nova lei estava realizando, foi desenvolvida a LGPD, como uma espécie de versão brasileira das normas europeias, que fosse capaz de tratar os dados pessoais de forma mais abrangente que o Marco Civil da Internet[2].

Ao analisar o pré-projeto da LGPD, Fortes (2016) já a comparava com as leis europeias e considerava que a lei brasileira possuía uma maior abrangência sobre a matéria. De fato,

> Por análise comparativa das diretivas europeias, verifica-se que o rol de definições do anteprojeto de lei dos dados pessoais é significativo e consistente para abranger diversas hipóteses fáticas, relacionadas ao que o anteprojeto define como tratamento de dados. Observa-se também que o anteprojeto brasileiro recepciona o conceito do consentimento como um dos elementos de tutelados dados pessoais (FORTES, 2016)

Em seu Artigo 1º, a Lei Geral de Proteção de Dados delimita sua finalidade, na qual procura através de diversos artifícios jurídicos, regular a forma em que os dados pessoais são administrados, com o intuito de sempre respeitar os direitos individuais, realizando o tratamento de forma responsável e transparente.

> O objetivo da LGPD é o de "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade natural". O verbo "proteger" diz muito sobre a forma como o legislador enxergou o titular dos dados, ou seja, em posição desigual em relação aos responsáveis pelo tratamento de dados, ficando patente sua vulnerabilidade (COTS; OLIVEIRA, 2018)

[2] Lei n. 12.965/14, responsável por regular o uso da *internet* no Brasil, através da imposição de princípios, direitos e deveres aos usuários da rede, bem como determinação de normas a serem seguidas pelo Estado.

Reconhecendo que a grande maioria dos cidadãos não compreende como é feita a coleta e o tratamento de seus dados, a LGPD se dispõe a cuidar da proteção dos dados de todas as pessoas, naturais ou jurídicas, levando em consideração todos os tipos de interações, das mais simples às mais avançadas, já que as tecnologias se fazem presente de forma integral na vida de grande parte da população.

2.4 Dados na Visão da LGPD

No Artigo 5º da lei é revelada a importância de sua utilização, onde nele são definidos o que a LGPD irá proteger durante o tratamento dos dados.

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; [...] (BRASIL, 2018)

É importante ressaltar que a definição de dado pessoal não se restringe a uma informação vaga, mas sim a qualquer informação que possa identificar uma pessoa dentro de um grupo. Quando sensível, refere-se a informações muitas vezes de cunho pessoal, que dependem exclusivamente da personalidade do cidadão. Para exemplificar, pode-se citar como dado pessoal, as compras que determinada pessoa realizou na *internet*, enquanto um dado sensível poderia ser sua preferência política, que está intimimamente relacionada à sua personalidade, experiências de vida, ciclo social etc.

Já o dado anonimizado, refere-se àqueles dados que foram submetidos a processos que deixaram o titular anônimo, podendo ser também dados genéricos e estatísticos, como por exemplo, pesquisas baseadas em médias de idade. Esses dados não são regulados pela LGPD.

2.5 A lei exige a Segurança dos Dados

No artigo 6º da LGPD, podem ser vistas as exigências sobre a maneira em que os dados são abordados, enumerando-se todos os princípios a serem respeitados quando se refere a assuntos sensíveis da população, nesse caso, os dados pessoais.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Dentre todos os princípios abordados nesse artigo, o princípio da segurança é um dos mais importantes, pois, é nele em que a LGPD exige do operador[3] que os métodos de segurança sejam reforçados e a integridade dos dados, assim como de seus processos, seja mantida, resultando em um ambiente seguro para o tratamento de informações. Destaca-se que o não cumprimento dessas regras pode causar a imposição de sanções por meio da Autoridade Nacional de Proteção de Dados (ANPD).

2.6 Autoridade Nacional de Proteção de Dados

Após a publicação da LGPD, criou-se a Autoridade Nacional de Proteção de Dados (ANPD), com sua competência estabelecida no art. 55-J, cujas funções principais são: garantir a aplicação da lei, realizar a sua fiscalização, comunicar-se com os controladores[4] e aplicar as sanções em casos em que forem reconhecidas irregularidades.

A Autoridade Nacional de Proteção de Dados (ANPD) é uma autarquia vinculada ao Ministério da Justiça e Segurança Pública do Brasil, criada pela Lei nº 13.709, de 14 de agosto

[3] "Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;" (art. 5º inciso VI, LGPD).
[4] Controladores são definidos pela LGPD, em seu Artigo 5º, como "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

de 2018 (BRASIL, 2018). A ANPD tem como missão zelar pela proteção de dados pessoais, orientar, regulamentar e fiscalizar o cumprimento da legislação. A ANPD foi estabelecida para implementar a LGPD, que visa garantir o direito de todos os brasileiros terem seus dados pessoais devidamente protegidos (BRASIL, 2018).

A ANPD possui autonomia técnica e decisória, com patrimônio próprio, e é responsável por elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade. Além disso, a ANPD promove a disseminação de conhecimentos sobre as normas e políticas públicas relacionadas à proteção de dados pessoais e às medidas de segurança. A ANPD também fiscaliza e aplica sanções em caso de tratamento de dados realizado em descumprimento à legislação.

A Autoridade pode instaurar processos de fiscalização para investigar o tratamento de dados pessoais sensíveis, como informações biométricas, e solicitar informações detalhadas das empresas envolvidas. A ANPD busca garantir que os dados pessoais sejam tratados de forma transparente e segura, protegendo a privacidade dos cidadãos. A LGPD, por sua vez, estabelece normas rigorosas para o tratamento de dados pessoais, incluindo dados biométricos, como a íris dos olhos.

2.7 Sanções previstas na LGPD

No que diz respeito a punições, a LGPD se divide em dois mecanismos. O primeiro deles é a responsabilização administrativa através da aplicação de sanções pela ANPD. Já o segundo, é a responsabilização civil e reparação de danos por meio de indenização, através do Judiciário (MONTEIRO, 2019).

Quanto à aplicação de sanções, a lei delimita que esse procedimento se trata de uma competência exclusiva da ANPD e deve ser realizado ao término de procedimentos administrativos, incluindo o direito a defesa. As sanções podem ser advertências, publicização da infração, bloqueio e eliminação de dados pessoais ou multas simples de até 2% (dois por cento) do faturamento com limite de R$ 50.000.000,00 (cinquenta milhões de reais), levando em consideração os parâmetros fixados no art. 52, § 1º:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
> I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;
> II - a boa-fé do infrator;

> III - a vantagem auferida ou pretendida pelo infrator;
> IV - a condição econômica do infrator;
> V - a reincidência;
> VI - o grau do dano;
> VII - a cooperação do infrator;
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
> IX - a adoção de política de boas práticas e governança;
> X - a pronta adoção de medidas corretivas; e
> XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

É importante levar em consideração quando o problema está relacionado a outros órgãos públicos sancionadores, considerando qeu, em eventuais irregularidades cometidas durante o tratamento de dados, serão realizadas fiscalizações e punições pela ANPD e não pelo órgão envolvido. Cita-se como exemplo a previsão realizada nos Artigos 55-J, § 2º e 55-K, sobre a atuação conjunta da ANPD com outras entidades públicas que realizam a regulação de determinados setores, além do Sistema Nacional de Defesa do Consumidor.

Logo, o processo administrativo pode ser visto como indispensável para a realização de apurações sobre atos irregulares, onde o acusado sofreria um processo, seguindo todos os seus direitos garantidos pela Constituição, incluindo apresentar sua defesa, antes que qualquer decisão seja tomada (BRASIL, 1999).

2.8 Política de Segurança da Informação na LGPD

A partir das normas a serem seguidas, a LGPD define em seu texto a importância do emprego de padrões técnicos, com o objetivo de facilitar o controle dos dados pessoais. Atendendo a especificações como o estabelecimento de regras de boa prática, capazes de serem aplicadas a todos os conjuntos de dados, de forma adaptável e que transmitam confiança aos titulares.

No entanto, a lei nº 13.709/18, em seu artigo 50, não define padrões a serem utilizados pelas organizações, apenas o que eles devem atender. O texto afirma que as regras de boa prática e de governança dispostas nas organizações podem ser reconhecidas e divulgadas pela autoridade nacional, além disso, sua adoção será estimulada pela mesma (BRASIL, 2018).

Baseando-se nisso, propõe-se a apresentação e construção de um modelo padrão de Política de Segurança da Informação. Esse documento reúne um conjunto de técnicas que devem ser transmitidas a todos os envolvidos no tratamento de dados e é capaz de atender as exigências impostas pela LGPD, seguindo os princípios da adaptabilidade e proteção, exigidos pela lei.

3 METODOLOGIA

O trabalho foi construído com base em pesquisas exploratórias relacionadas ao tema, utilizando abordagens qualitativas de conteúdos e conceitos necessários para a sua elaboração. A partir dessas pesquisas, foi desenvolvido um modelo de política, resultado da compilação aplicada aos estudos feitos.

Em sua construção foram empregados recursos do Microsoft® Office, apresentando e explicando o modelo construído por meio de uma apreciação visual do documento. Cada momento é acompanhado de suas respectivas explicações, permitindo a reprodução do método a partir de sua observância.

Como a intenção é disponibilizar o resultado do trabalho, optou-se pela utilização do Office 2007, mesmo tendo conhecimento de que esta versão é antiga, a fim de garantir que a execução dos processos seja possível também em versões mais atualizadas do Pacote (por meio da retrocompatibilidade), buscando desta forma ampliar o escopo da possibilidade de utilização da documentação proposta. A escolha de uma versão mais recente poderia, em algum momento, impedir que possíveis instalações de versões anteriores dos *softwares* fossem desqualificadas para usar o método apresentado neste trabalho.

Para que a composição dos documentos alcance uma percepção mais próxima de sua aplicação prática, forão utilizados dados fictícios para o preenchimento das variáveis que fazem parte da construção dos modelos. Os documentos gerados no desenvolvimento deste trabalho serão disponibilizados para *download*, permitindo sua utilização para quem se interessar na sua aplicação prática.

O desenvolvimento deste trabalho baseia-se, em um primeiro momento na construção de um texto-base que possa ser utilizado como Modelo de uma Política de Segurança da Informação (PSI). Sua construção ocorreu através do estudo sobre os conceitos expostos no capítulo Revisional Teórico e também de observações diversas a documentos pré-estabelecidos e disponíveis para consulta na internet (ANPD, 2021).

Os tópicos utilizados neste modelo seguem uma construção estabelecida a critério de autoria, sendo considerados os seguintes componentes:

- Segurança quanto às Pessoas;
- Segurança quanto aos Sistemas;
- Segurança da Web;
- Suporte;
- Termo de Responsabilidade.

Cada um dos componentes listados recebe abordagem específica quanto à sua contribuição para a PSI proposta.

4 DESENVOLVIMENTO

Neste capítulo, apresenta-se a aplicação prática do modelo de Política de Segurança da Informação (PSI) elaborado com base nos conceitos explorados no referencial teórico e nas metodologias descritas anteriormente. A proposta é detalhar cada componente do modelo, explicando como ele contribui para atender às exigências da LGPD e promover a segurança no tratamento de dados sensíveis.

O desenvolvimento contempla cinco tópicos principais: Segurança quanto às Pessoas, Segurança quanto aos Sistemas, Segurança da Web, Suporte e o Termo de Responsabilidade. Cada tópico é analisado de forma a oferecer uma visão clara das medidas e práticas que devem ser implementadas, além de destacar as partes adaptáveis do modelo, permitindo sua aplicação em diferentes organizações.

4.1 Segurança quanto às Pessoas

Este trecho da PSI, ilustrado na Figura 01, diz respeito às regras a serem atendidas em relação aos funcionários das organizações e apresenta a metodologia a ser aplicada para que os mesmos possuam conhecimento sobre as normas e punições.

Figura 01: Regras de Segurança em relação às Pessoas.

I. Segurança quanto às Pessoas

a) **Identificação de Pessoas**

- Todos os colaboradores que possuírem acesso aos sistemas, devem ter uma identificação única (*login*).

b) **Declaração de Responsabilidade**

- Os colaboradores devem ler atentamente as Políticas de Segurança da empresa e assinar o Termo de Responsabilidade, comprovando que estão cientes das normas a serem seguidas e que o não cumprimento das mesmas poderá ocasionar punições disciplinares internas e/ou ações penais previstas em lei.

Fonte: Elaborado pelo autor, 2021.

Na letra ‘a)’ é contemplada a forma de acesso ao sistema para cada um dos colaboradores, a ideia é utilizar-se de uma prática comum de identificação, o *login*, que permite a cada usuário um acesso único contendo somente as tarefas e os dados que lhe cabem por função, além da segurança de uma senha. Dessa forma o acesso de pessoas não autorizadas a Dados Sensíveis se tornaria impossível, desde que todos os cuidados sejam tomados.

Enquanto o tópico da letra ‘b)’ se certifica que os usuários estejam cientes das diretrizes que estão vigentes em seu meio profissional, bem como as suas punições em caso de descumprimento. Pensando nisso, foi idealizado um Termo de Responsabilidade complementar a PSI e que deve ser assinado por todos os colaboradores.

4.2 Segurança quanto aos Sistemas

Neste trecho, a prioridade são os sistemas. Afinal, para a segurança dos dados, os cuidados com estes são primordiais. Por esse motivo, os sistemas devem estar sempre atualizados e tal necessidade é contemplada na PSI proposta, conforme apresentado na Figura 02.

Figura 02: Cuidados para com os Sistemas.

II. Segurança quanto aos Sistemas

a) **Sistemas**

- Os sistemas devem estar sempre atualizados, principalmente nos requisitos de segurança.
- Equipamentos portáteis (*notebooks*, *tablets* e *smartphones*) que possam ser utilizados para o armazenamento de dados, devem ser protegidos e atender as especificações de segurança impostas pela empresa, como a utilização da criptografia e acesso protegido por senha.
- É vetado o armazenamento de dados sigilosos em equipamentos particulares.

Fonte: Elaborado pelo autor, 2021.

O primeiro tópico exibe as ações a serem tomadas pela organização e seus funcionários, incluindo tarefas como o uso de equipamentos e *softwares* autorizados, o emprego de senhas e criptografias, e o veto de ações como armazenamento de dados em dispositivos particulares. Já o tópico visto na Figura 03, refere-se ao acesso dos usuários aos sistemas:

Figura 03: Acessos Permitidos.

b) **Acesso dos Usuários**

- Além do acesso permitido aos colaboradores, devem ser contempladas as atividades de adição e exclusão de contas. Se um colaborador for demitido ou mudar de setor dentro da organização, seu *login* deve ser excluído e no segundo caso, deverá ser criado um novo acesso, correspondente a sua nova função.

Fonte: Elaborado pelo autor, 2021.

Como citado, somente pessoas autorizadas podem fazer o uso dos sistemas e de seus dados, sendo assim, o acesso de colaboradores que forem demitidos ou promovidos a novos cargos deve ser removido, uma vez que os conteúdos antes fornecidos, não podem ser utilizados por eles, garantindo assim o controle e a privacidade que a PSI busca apoiar.

No que tange a utilização de senhas, a Figura 04 apresenta a parte da PSI proposta que aborda esta situação.

Figura 04: Cuidados sobre as Senhas.

c) **Senhas**

- As senhas consideradas seguras deverão conter ao menos 08 (oito) caracteres alfanuméricos (letras e números), mesclando letras minúsculas e maiúsculas;
- Cada senha possuirá um prazo de validade de 30 (trinta) dias, se excedido, o acesso será bloqueado;
- Caso o sistema apresente uma senha inicial, é obrigatória a sua alteração, no primeiro acesso;
- Se o máximo de 04 (quatro) tentativas consecutivas de acesso for atingido, os acessos devem ser impedidos até que o usuário solicite o desbloqueio.

Fonte: Elaborado pelo autor, 2021.

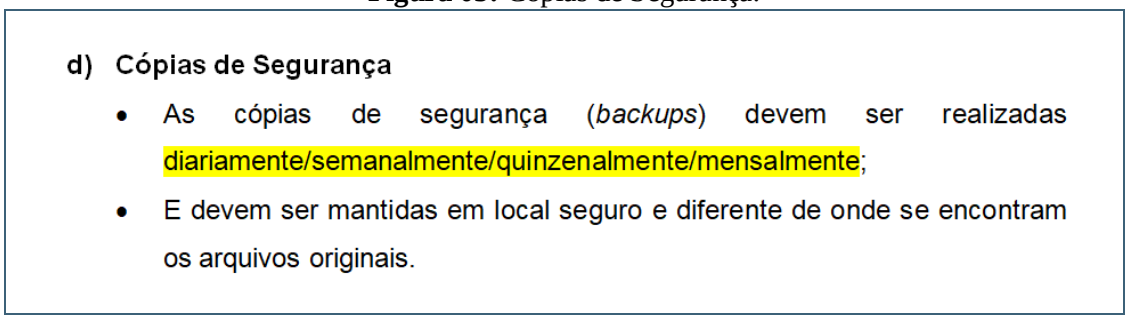
Diferente dos demais tópicos, esse é constituído de conteúdos em destaque, que serão tratados no trabalho como sendo adaptáveis. Isso ocorre porque, mesmo com a PSI sendo majoritariamente padronizada, alguns de seus itens irão sempre variar de empresa para empresa. Portanto, cabe a cada uma definir individualmente o número de caracteres presentes na senha e sua composição, o prazo de validade delas, se a sua alteração inicial é obrigatória ou opcional e o número de tentativas de acesso que cada usuário poderá ter. Alternativamente, poderão optar por algum dos modelos pré-definidos na PSI.

O tratamento de senhas é uma situação comum na utilização de sistemas informatizados em geral, porém ganha relevância no ambiente empresarial devido a todo o contexto de

proteção dos dados. Tais exigências apresentadas nesta proposta de PSI podem, em algum momento, significar algum desconforto por parte dos usuários, mas trata-se de ações importantes para combater o envelhecimento das senhas utilizadas (MACHADO, 2014).

Em relação às cópias de segurança (*backups*), assim como as definições sobre as senhas, cada organização adota seu próprio cronograma de realização. Por isso, entende-se que este conteúdo seja adaptável como visto na Figura 05. Este elemento recebe algumas opções já parametrizadas, sendo elas as mais comuns dentre as presentes em Políticas de Segurança da Informação na *internet* (ANPD, 2021)

Figura 05: Cópias de Segurança.


d) **Cópias de Segurança**

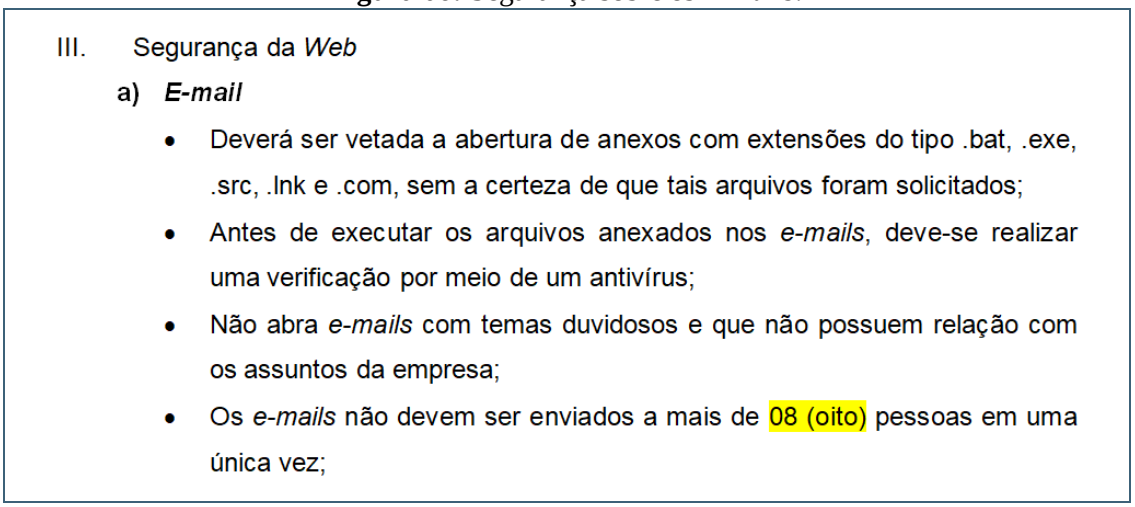
- As cópias de segurança (*backups*) devem ser realizadas diariamente/semanalmente/quinzenalmente/mensalmente;
- E devem ser mantidas em local seguro e diferente de onde se encontram os arquivos originais.

Fonte: Elaborado pelo autor, 2021.

4.3 Segurança da *Web*

Em relação à Segurança na *Web*, o tema recebeu atenção em dois itens. O primeiro deles diz respeito aos cuidados sobre os *e-mails*, que mostra aos leitores as ações que devem tomar quando receberem ou enviarem mensagens por correio eletrônico.

Figura 06: Segurança sobre os *E-mails*.


III. Segurança da *Web*

a) ***E-mail***

- Deverá ser vetada a abertura de anexos com extensões do tipo .bat, .exe, .src, .lnk e .com, sem a certeza de que tais arquivos foram solicitados;
- Antes de executar os arquivos anexados nos *e-mails*, deve-se realizar uma verificação por meio de um antivírus;
- Não abra *e-mails* com temas duvidosos e que não possuem relação com os assuntos da empresa;
- Os *e-mails* não devem ser enviados a mais de 08 (oito) pessoas em uma única vez;

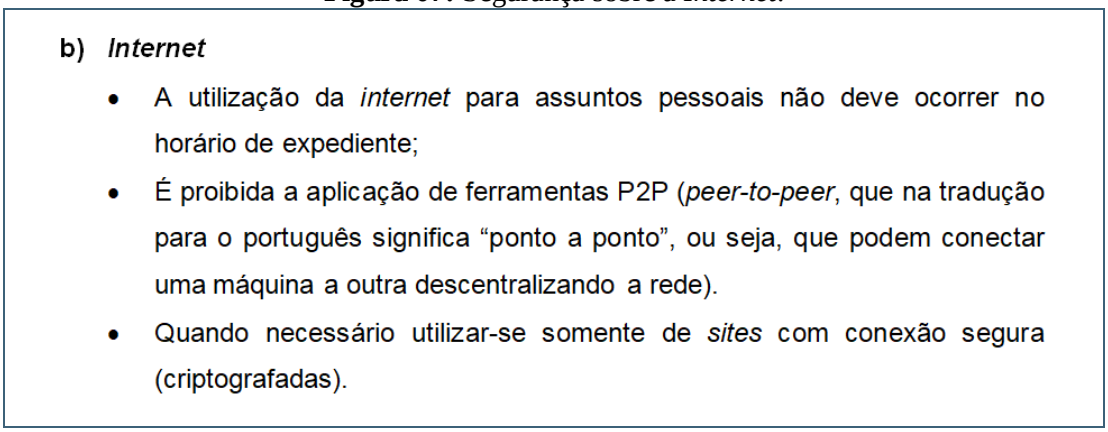
Fonte: Elaborado pelo autor, 2021.

Como visto na Figura 06, ações como aberturas de anexos com extensões autoexecutáveis com temas que não condizem com os trabalhados da empresa devem ser completamente vetados e quando os arquivos forem solicitados devem passar por uma análise

de um antivírus de qualidade. Neste item, também se encontra mais um conteúdo adaptável, referente ao número máximo de pessoas atribuídas na lista de distribuição de mensagens (no exemplo, o limite é de oito pessoas, mas a quantia final ficará a critério de cada organização).

Além do tópico *e-mail*, o outro ponto destacado na Figura 07 está relacionado à *internet*, por ser um dos recursos mais utilizados da tecnologia, estando presente em todas as organizações atuais (SOARES; DA SILVA SOARES; ALVES, 2021).

Figura 07: Segurança sobre a *Internet*.



Fonte: Elaborado pelo autor, 2021.

Neste tópico a atenção foi voltada a como os funcionários devem se comportar durante a jornada de trabalho, evitando a utilização da *internet* para outros fins que não sejam referentes à sua função, aplicações de ferramentas que descentralizem a rede e navegação em *sites* sem conexão segura.

4.4 Suporte

Para finalizar a PSI proposta, foi acrescido um campo para informar os dados de pessoas que compõem as Equipes técnica e de segurança, como pode ser visualizado na Figura 08:

Figura 08: Contatos para Suporte.

IV. Suporte

Em caso de dúvidas, entre em contato com a equipe técnica ou com a equipe de segurança.

a) **Equipe Técnica**

Nome	E-mail	Celular	Ramal
Nome Sobrenome	nome@empresa.com	(XX) XXXXX-XXXX	###

b) **Equipe de Segurança**

Nome	E-mail	Celular	Ramal
Nome Sobrenome	nome@empresa.com	(XX) XXXXX-XXXX	###

Fonte: Elaborado pelo autor, 2021.

Os quadros são constituídos por campos personalizáveis, onde estarão os nomes dos colaboradores pertencentes aos respectivos setores, assim como seus demais dados (*e-mail*, celular e ramal). Uma versão completa da PSI que foi proposta poderá ser apreciada no Anexo 01 deste trabalho.

4.5 Termo de Responsabilidade

Para se garantir a ciência dos colaboradores em relação à PSI implantada na organização, idealizou-se um Modelo de Termo de Responsabilidade que indica os deveres dos envolvidos, bem como as possíveis sanções que poderão sofrer, em caso de descumprimento das ações.

Figura 09: Cabeçalho do Termo.

ANEXO 02 – MODELO DE TERMO DE RESPONSABILIDADE

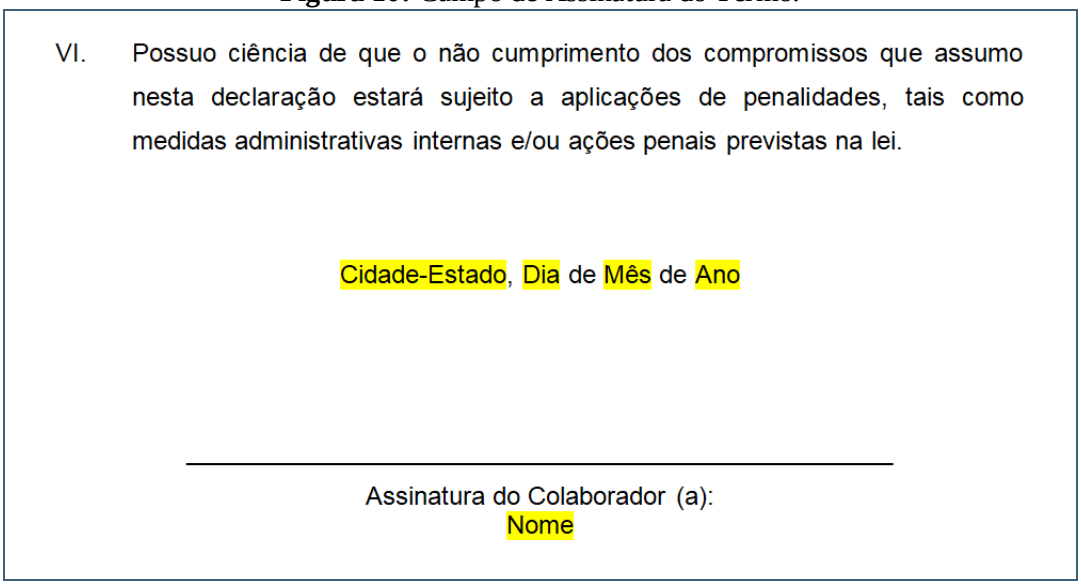
Eu, Nome, portador (a) do CPF Nº NumCPF, declaro estar ciente sobre as normas e responsabilidades regidas pela Política de Segurança da Informação, entregue a mim pela NomeDaEmpresa, inscrita no CNPJ NumCNPJ e localizada na Endereço. Afirmo ter lido e adquirido o conhecimento sobre as seguintes responsabilidades:

I. Os acessos às informações e instalações fornecidos a mim pela empresa, estarão sobre minha responsabilidade durante até o momento de meu desligamento;

Fonte: Elaborado pelo autor, 2021.

Em seu cabeçalho (Figura 09) encontram-se campos adaptáveis, nos quais serão informados os dados dos Colaboradores e da Empresa onde atua.

Figura 10: Campo de Assinatura do Termo.



VI. Possuo ciência de que o não cumprimento dos compromissos que assumo nesta declaração estará sujeito a aplicações de penalidades, tais como medidas administrativas internas e/ou ações penais previstas na lei.

Cidade-Estado, Dia de Mês de Ano

Assinatura do Colaborador (a):
Nome

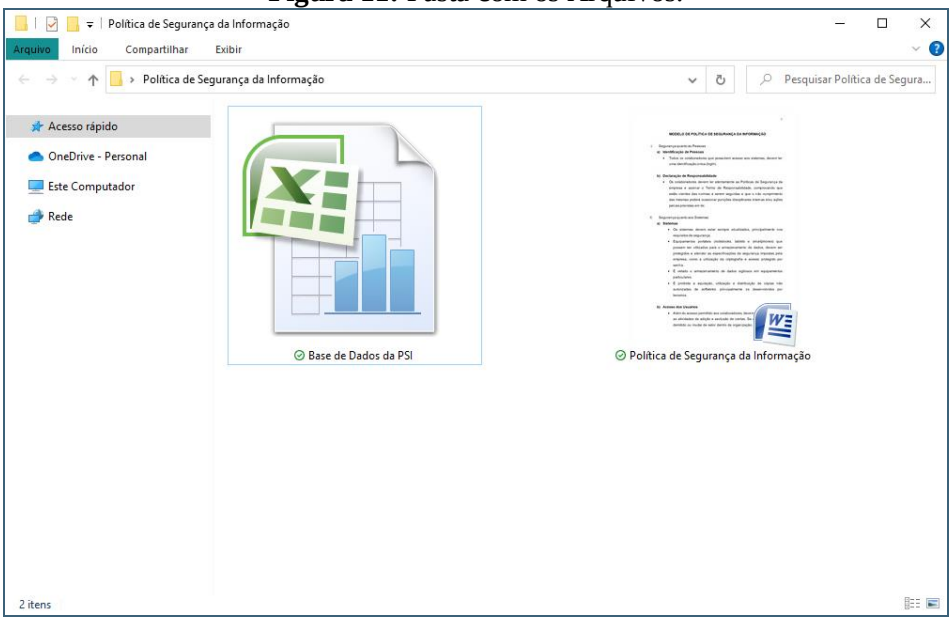
Fonte: Elaborado pelo autor, 2021.

O Termo finaliza com espaços para acréscimo de dados como cidade e estado, data e a assinatura do colaborador que o recebeu (Figura 10). O Termo deverá ser entregue em conjunto da PSI, como documentação única e que assegure o entendimento de ambas as partes (Organização e Funcionários). E assim como a Política de Segurança da Informação, o Termo possui uma versão completa que poderá ser visualizada no Anexo 02.

4.6 Processo de Montagem da PSI

Após o desenvolvimento de todo o documento da PSI juntamente de seu Termo de Responsabilidade, deu-se início a etapa seguinte, o desenvolvimento prático sobre os conteúdos adaptáveis. Conforme exposto na Metodologia do trabalho todas as ações realizadas para esse desenvolvimento utilizaram-se de recursos pertencentes ao Microsoft® Office 2007, para se valer da retrocompatibilidade presente em versões mais atuais dos *softwares*.

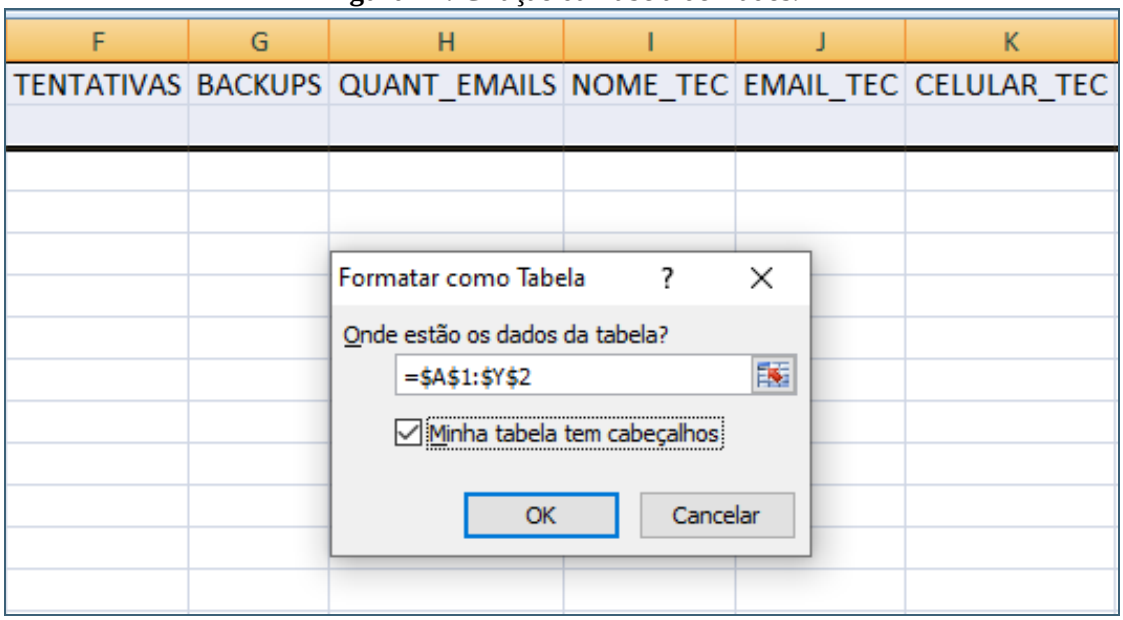
Figura 11: Pasta com os Arquivos.



Fonte: Elaborado pelo autor, 2021.

Para facilitar a construção, foi criada uma pasta na área de trabalho do computador utilizado (Figura 11), e nela foram anexados dois arquivos: o documento da Política de Segurança da Informação e uma planilha do Excel denominada Base de Dados da PSI. A planilha foi aberta e deu se iniciou aos seguintes processos:

Figura 12: Criação da Tabela de Dados.



Fonte: Elaborado pelo autor, 2021.

Após a sua abertura, foi construída uma tabela de dados similar à de interfaces presentes em Bancos de Dados, sendo o motivo pelo qual cada conteúdo adaptável foi vinculado a uma variável (Figura 12). Ao término da construção de seu ‘esqueleto’, foi escolhido um estilo de

formatação (nesse caso o 'Estilo de Tabela Média 15'), ao escolher um tema, o sistema exibe a mensagem presente na figura acima. Deve-se marcar que a tabela tem cabeçalhos e finalizar clicando no botão 'OK'.

Figura 13: Versões de Adaptações Desenvolvidas.

ID	NUM_SENHA	CHAR_SENHA	VAL_SENHA	ALT_SENHA1	TENTATIVAS	BACKUPS	QUANT_EMAILS
1	08 (oito)	numéricos (números)	15 (quinze) dias	obrigatória	04 (quatro)	diariamente	05 (cinco)
2	06 (seis)	alfanuméricos (letras e números), mesclando letras minúsculas e maiúsculas	30 (trinta) dias	obrigatória	05 (cinco)	semanalmente	05 (cinco)
3	10 (dez)	alfabéticos (letras), mesclando letras minúsculas e maiúsculas	15 (quinze) dias	obrigatória	06 (seis)	quinzenalmente	05 (cinco)
4	06 (seis)	numéricos (números)	30 (trinta) dias	opcional	05 (cinco)	mensalmente	08 (oito)
5	10 (dez)	alfanuméricos (letras e números), mesclando letras minúsculas e maiúsculas	15 (quinze) dias	opcional	06 (seis)	diariamente	08 (oito)
6	06 (seis)	alfabéticos (letras), mesclando letras minúsculas e maiúsculas	30 (trinta) dias	opcional	04 (quatro)	semanalmente	08 (oito)
7	12 (doze)	numéricos (números)	15 (quinze) dias	obrigatória	07 (sete)	quinzenalmente	10 (dez)
8	12 (doze)	alfanuméricos (letras e números), mesclando letras minúsculas e maiúsculas	30 (trinta) dias	obrigatória	07 (sete)	mensalmente	10(dez)
9	08 (oito)	alfabéticos (letras), mesclando letras minúsculas e maiúsculas	15 (quinze) dias	obrigatória	05 (cinco)	diariamente	10 (dez)
10	10 (dez)	numéricos (números)	30 (trinta) dias	opcional	06 (seis)	semanalmente	03 (três)
11	08 (oito)	alfanuméricos (letras e números), mesclando letras minúsculas e maiúsculas	15 (quinze) dias	opcional	04 (quatro)	quinzenalmente	03 (três)
12	12 (doze)	alfabéticos (letras), mesclando letras minúsculas e maiúsculas	30 (trinta) dias	opcional	07 (sete)	mensalmente	03 (três)

Fonte: Elaborado pelo autor, 2021.

No passo seguinte, ilustrado na Figura 13, a tabela foi nomeada e a ela foram atribuídos dados fictícios para exemplificar como os processos ocorrem. Em relação às variações de personalização foram criadas 12 combinações de modelos diferentes, constituídas por: números de caracteres possíveis para as senhas (06 dígitos, 08 dígitos, 10 dígitos e 12 dígitos), tipos de caracteres (numéricos, alfanuméricos e alfabéticos), validades para as senhas (15 dias e 30 dias), alteração de senha inicial (obrigatória e opcional), tentativas de acesso (04 tentativas, 05 tentativas, 06 tentativas e 07 tentativas), períodos de realização das cópias de segurança – *backups* (diariamente, semanalmente, quinzenalmente e mensalmente) e quantidade limite de envios de *e-mails* (03 cópias, 05 cópias, 08 cópias e 10 cópias).

Os demais dados referentes à Equipe Técnica e a Equipe de Segurança, foram divididos como se cada setor possuísse dois funcionários e cada um deles fosse responsável por metade das versões do modelo, estando presentes seus respectivos dados (*e-mail*, celular e ramal), como pode ser visto na Figura 14.

Figura 14: Equipe Técnica e Equipe de Segurança.

NOME_TEC	EMAIL_TEC	CELULAR_TEC	RAMAL_TEC	NOME_SEG	EMAIL_SEG	CELULAR_SEG	RAMAL_SEG
Ednaldo Pereira	ednaldo@snow.com	(00) 1 1176-5432	433	Henrique Freecs	henrique@snow.com	(00) 1 1132-7654	405
Ednaldo Pereira	ednaldo@snow.com	(00) 1 1176-5432	433	Henrique Freecs	henrique@snow.com	(00) 1 1132-7654	405
Ednaldo Pereira	ednaldo@snow.com	(00) 1 1176-5432	433	Henrique Freecs	henrique@snow.com	(00) 1 1132-7654	405
Ednaldo Pereira	ednaldo@snow.com	(00) 1 1176-5432	433	Henrique Freecs	henrique@snow.com	(00) 1 1132-7654	405
Ednaldo Pereira	ednaldo@snow.com	(00) 1 1176-5432	433	Henrique Freecs	henrique@snow.com	(00) 1 1132-7654	405
Ednaldo Pereira	ednaldo@snow.com	(00) 1 1176-5432	433	Henrique Freecs	henrique@snow.com	(00) 1 1132-7654	405
Antônio Carlos de Souza	antonio@snow.com	(00) 1 1167-2543	485	Augusto Braga	augusto@snow.com	(00) 1 1123-4657	409
Antônio Carlos de Souza	antonio@snow.com	(00) 1 1167-2543	485	Augusto Braga	augusto@snow.com	(00) 1 1123-4657	409
Antônio Carlos de Souza	antonio@snow.com	(00) 1 1167-2543	485	Augusto Braga	augusto@snow.com	(00) 1 1123-4657	409
Antônio Carlos de Souza	antonio@snow.com	(00) 1 1167-2543	485	Augusto Braga	augusto@snow.com	(00) 1 1123-4657	409
Antônio Carlos de Souza	antonio@snow.com	(00) 1 1167-2543	485	Augusto Braga	augusto@snow.com	(00) 1 1123-4657	409
Antônio Carlos de Souza	antonio@snow.com	(00) 1 1167-2543	485	Augusto Braga	augusto@snow.com	(00) 1 1123-4657	409

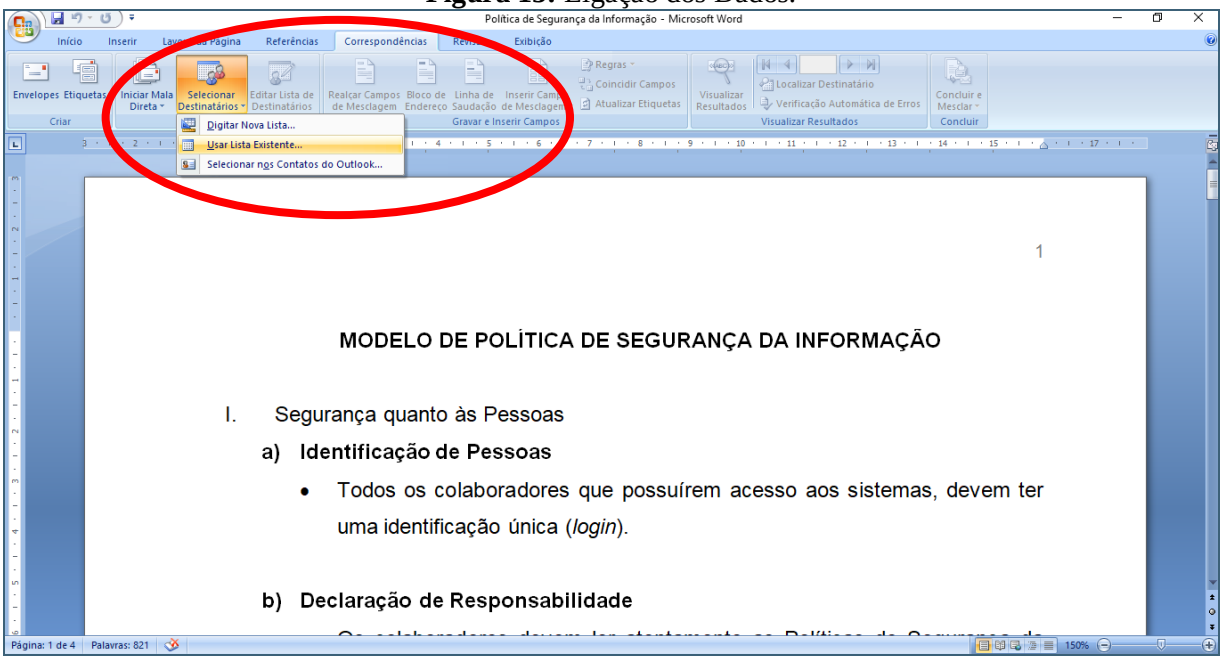
Fonte: Elaborado pelo autor, 2021.

No entanto, para que os Termos de Responsabilidade pudessem exibir dados de mais de um colaborador, essas ‘12 versões’ da PSI foram repetidas para que pudessem ser associadas a 04 pessoas, resultando em um número final de 48 *ID’s* presentes na tabela.

4.7 Associando os Dados do Excel ao Word

Com a tabela de dados pronta, a etapa seguinte foi a ligação entre o Excel e o Word. Para esse procedimento, foram necessárias as seguintes ações:

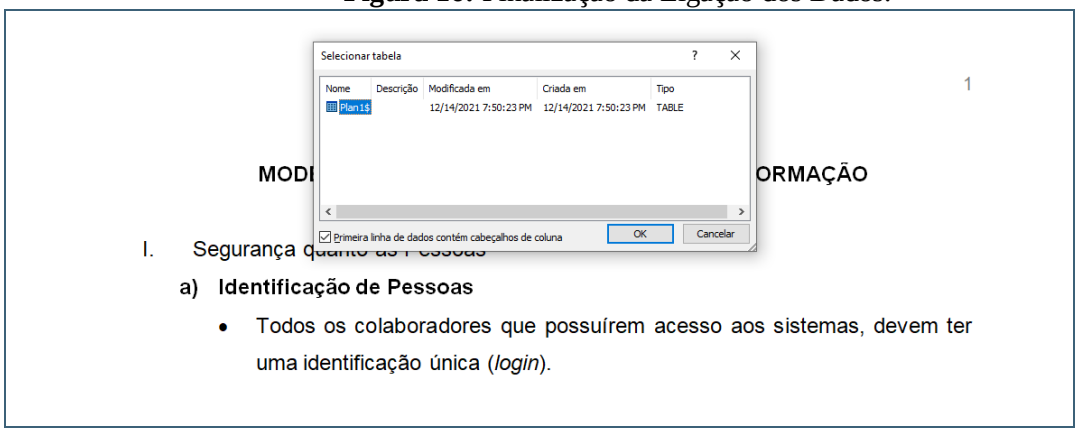
Figura 15: Ligação dos Dados.



Fonte: Elaborado pelo autor, 2021.

Como Visto na Figura 15, na aba ‘Correspondências’, o destinatário foi selecionado, neste caso era a lista já existente no arquivo denominado ‘Base de Dados da PSI’ (por isso a importância de que os documentos estejam em uma mesma pasta, para que seu encontro seja facilitado).

Figura 16: Finalização da Ligação dos Dados.



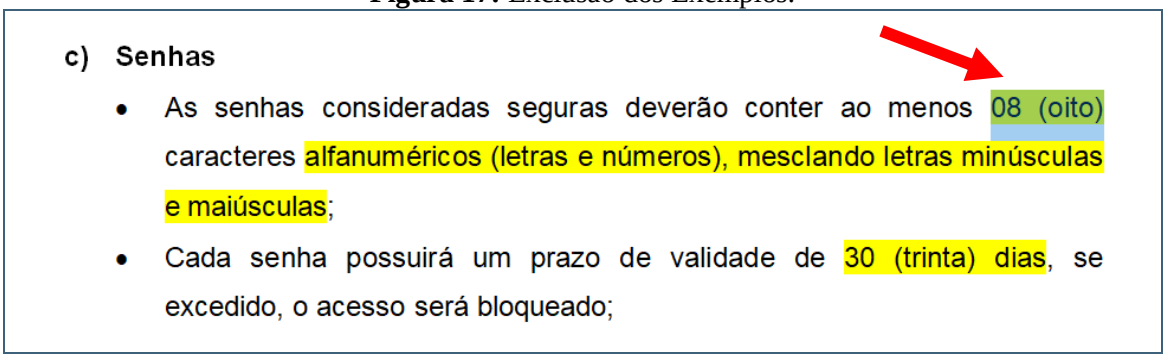
Fonte: Elaborado pelo autor, 2021.

Ao selecionar a fonte dos dados, a tela exibe a mensagem apresentada na Figura 16. Como há somente uma planilha existente no arquivo, ela deve ser selecionada, marcada a opção de que a primeira linha contém cabeçalhos e finalizado o processo com o botão 'OK'. Uma observação muito importante que merece destaque é que se em um documento, existirem mais de uma planilha, somente uma delas poderá ser associada ao Word, na tentativa de se adicionar uma segunda planilha ela irá se sobrescrever a anterior.

4.8 Substituição dos Conteúdos Adaptáveis

Para realizar a substituição dos conteúdos adaptáveis pelos dados presentes no Excel de forma automatizada, foram necessários dois passos bem simples:

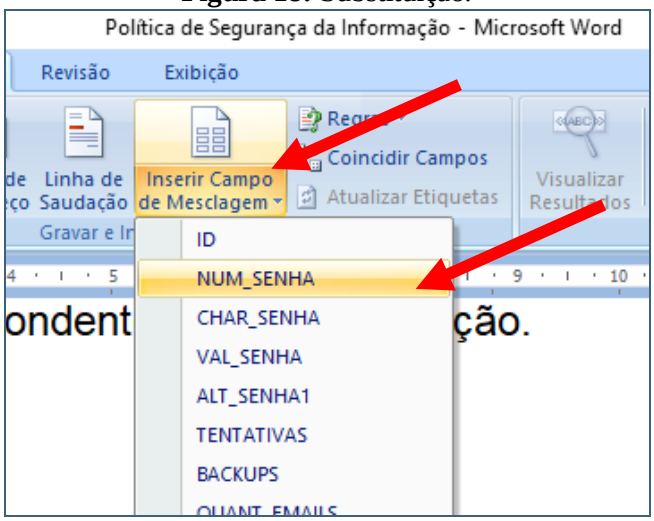
Figura 17: Exclusão dos Exemplos.



Fonte: Elaborado pelo autor, 2021.

Os dados que estavam marcados como exemplos no início do processo foram excluídos um a um como mostra a Figura 17. Com a exclusão dos trechos necessários, a inclusão das variáveis é feita conforme apresentado na Figura 18:

Figura 18: Substituição.



Fonte: Elaborado pelo autor, 2021.

Ainda na aba 'Correspondências', são habilitadas algumas opções após a ligação entre os arquivos, dentre elas a de Inserção de Campos de Mesclagem. Ao clicar nessa opção é possível visualizar todas as colunas presentes na planilha do Excel. É selecionada aquela que se encaixa na frase e o resultado obtido será visto como o exposto na Figura 19:

Figura 19: Resultado da Substituição.

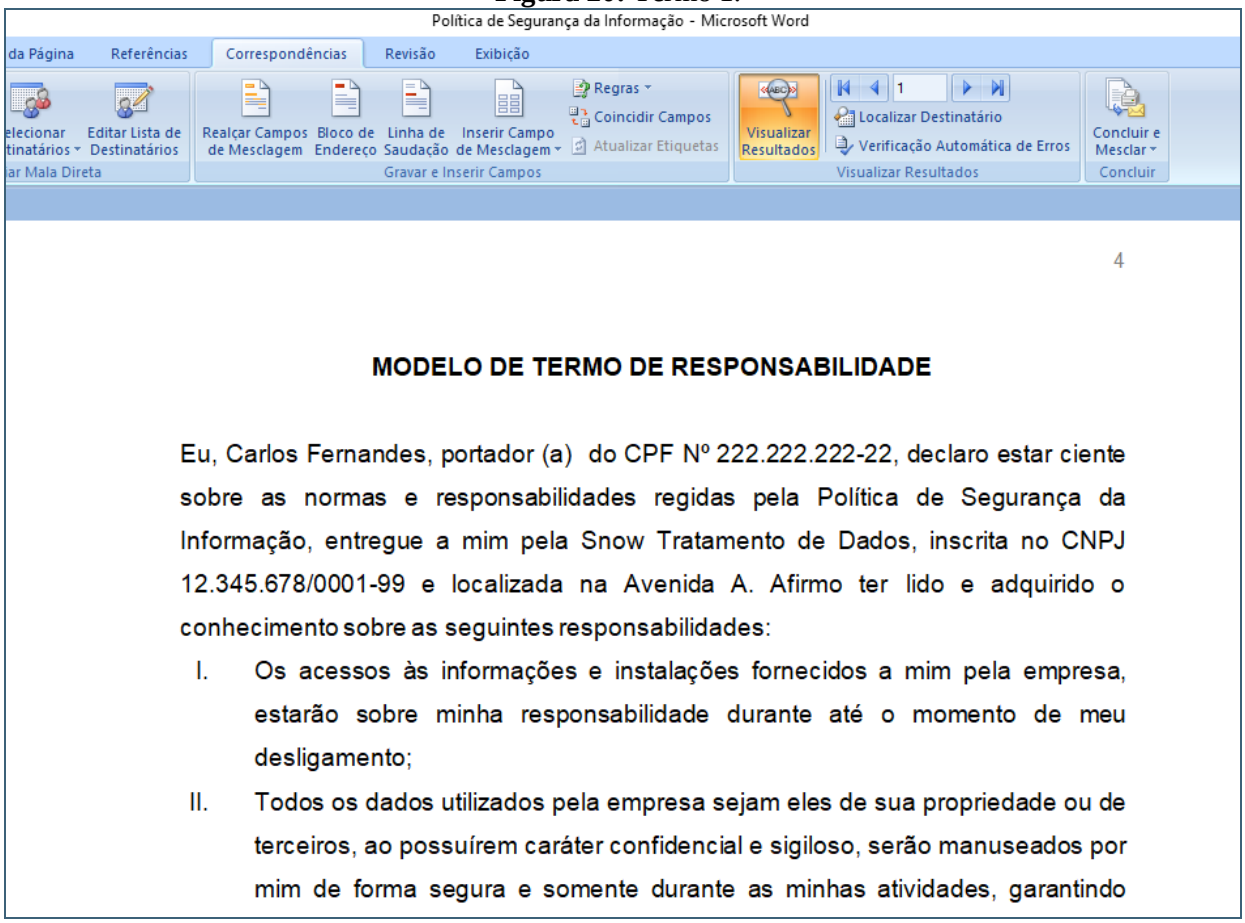
c) **Senhas**

- As senhas consideradas seguras deverão conter ao menos «NUM_SENHA» caracteres «CHAR_SENHA»;
- Cada senha possuirá um prazo de validade de «VAL_SENHA», se excedido, o acesso será bloqueado;
- Caso o sistema apresente uma senha inicial, é «ALT_SENHA1» a sua alteração, no primeiro acesso;
- Se o máximo de «TENTATIVAS» tentativas consecutivas de acesso for atingido, os acessos devem ser impedidos até que o usuário solicite o desbloqueio.

Fonte: Elaborado pelo autor, 2021.

Os locais que antes possuíam um marca-texto, agora possuem as variáveis dentro de símbolos de destaque. E assim foi feito por todo o corpo dos textos da PSI e do Termo de Responsabilidade, apresentado na Figura 20.

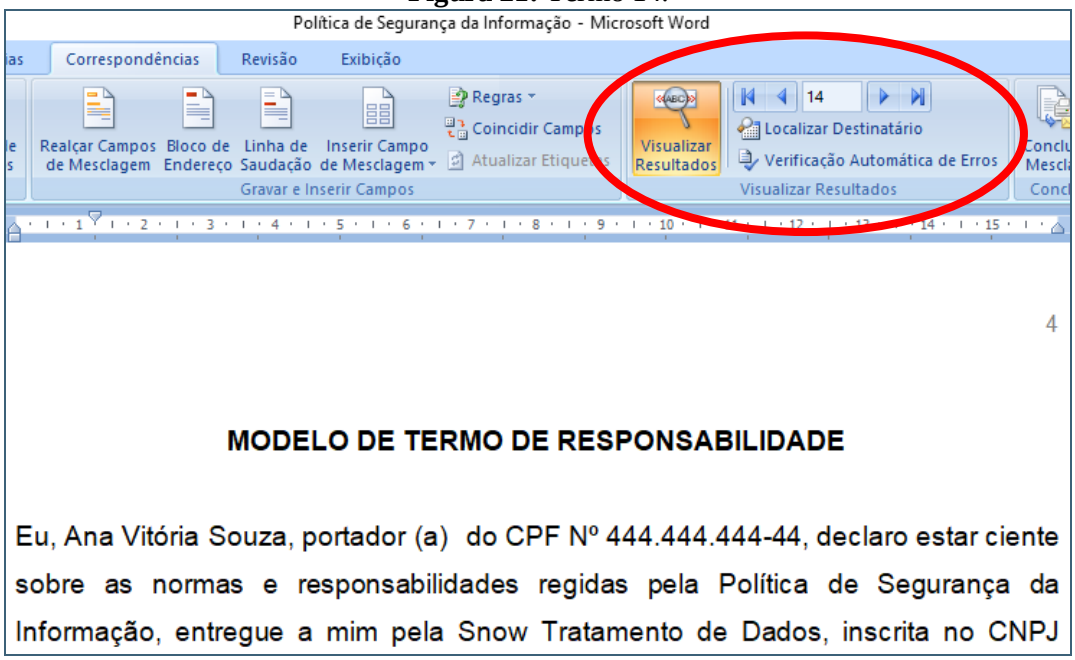
Figura 20: Termo 1.



Fonte: Elaborado pelo autor, 2021.

Para visualizar os dados e suas variações, é preciso clicar na opção ‘Visualizar Resultados’ da aba ‘Correspondências’ e navegar pelos os resultados anteriores e posteriores utilizando-se das setas presentes ou informando o número do ID específico que deseja. Na figura 20 está presente o Termo de Responsabilidade do ID 1, com o nome fictício de Carlos Fernandes, acompanhado de seu CPF. Já na figura 21, pode ser visto o Termo de Responsabilidade do ID 14, em nome de Ana Vitória Souza. E assim podem ser contemplados os resultados de ‘n documentos’.

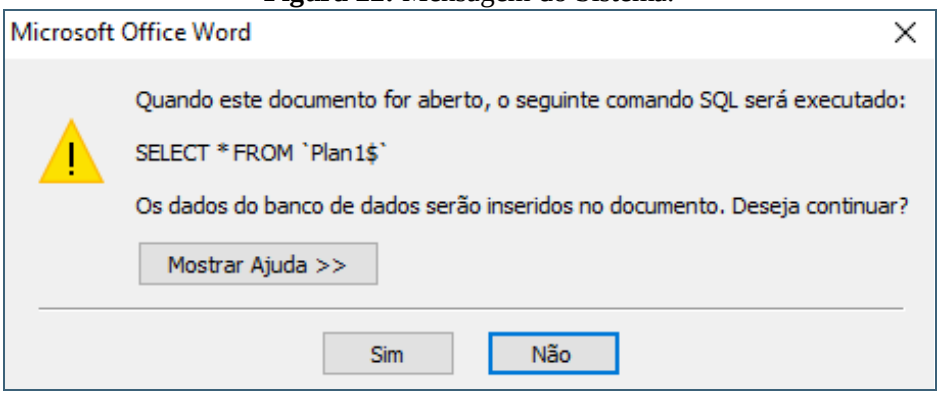
Figura 21: Termo 14.



Fonte: Elaborado pelo autor, 2021.

E sempre que o documento for aberto novamente, seja após atualizações, inserções ou exclusões de dados na Tabela do Excel, ou até mesmo para consultas do arquivo Word já existente, será exibida a mensagem apresentada na Figura 22:

Figura 22: Mensagem do Sistema.



Fonte: Elaborado pelo autor, 2021.

Nela deve-se clicar em ‘Sim’, para que os dados sejam sincronizados corretamente. Nota-se que a mensagem evidencia que o procedimento realizado entre o Excel e o Word, possui uma relação semelhante à de um Banco de Dados com uma Linguagem de Programação e a justificativa por trás de sua escolha foi exclusivamente a facilidade de acesso, já que o Pacote Office é reconhecidamente abrangente no que tange sua utilização em ambientes empresariais diversos.

Os arquivos gerados durante o desenvolvimento deste estudo foram disponibilizados para consulta e download na URL:

<https://drive.google.com/drive/folders/12QvEBEdfeWkJaU5bQ3QpYZJblsQWpyhC?usp=sharing>. Essa disponibilização visa permitir a reprodução do processo descrito no trabalho e facilitar a aplicação prática dos documentos, com as devidas adequações às necessidades específicas de cada organização, em conformidade com a LGPD. A prática de disponibilizar dados e materiais suplementares é reconhecida por promover a transparência e a reprodutibilidade científica (PIWOWAR et al., 2007; TENOPIR et al., 2011), aspectos fundamentais para o avanço do conhecimento científico.

5 CONSIDERAÇÕES FINAIS

O desenvolvimento do presente estudo possibilitou a elaboração de uma proposta de Política de Segurança da Informação, a partir das necessidades recentemente impostas pela Lei Geral de Proteção de Dados, visando oferecer um conhecimento mais estruturado para que as empresas possam, em algum nível, se adequar às exigências da lei, dada a importância no tratamento de dados pessoais, regulamentadas pela LGPD

Durante a realização das pesquisas, verificou-se que a importância de uma PSI para as organizações e colaboradores está sendo constantemente abordada, sendo inclusive apoiada pela ANPD, que em Outubro de 2021, disponibilizou um Guia Orientativo para Agentes de Tratamento, sugerindo a adoção de medidas administrativas como esta.

Tomando como base essas informações e demandas, idealizou-se a construção de dois documentos (uma ‘PSI’ e um ‘Termo de Responsabilidade’), ambos com espaços adaptáveis, capazes de receberem dados de qualquer empresa e seus respectivos colaboradores.

Para atingir esse resultado levaram-se em consideração três objetivos específicos: a apresentação de conteúdos que amparassem a construção de toda a documentação, o que se faz presente no capítulo do Referencial Teórico, atendendo concomitantemente ao segundo objetivo, de se filtrar os conteúdos considerados indispensáveis para uma PSI. E, por fim, as construções e apresentações dos materiais propostos, que podem ser contempladas no capítulo de Desenvolvimento.

A criação dos documentos levou em consideração a necessidade de acesso viável à sua reprodução, visto que o trabalho estabelece a premissa de que tais artefatos podem ser utilizados por uma gama variada de organizações. Deveu-se a isso a escolha dos *softwares* Excel e Word para a implementação do desenvolvimento, pois quanto mais simples fosse a construção dos documentos, melhor estaria apresentado o resultado proposto.

Os arquivos utilizados para a execução do processo apresentado no desenvolvimento estão disponíveis para *download* a todos os interessados, permitindo que o conhecimento

produzido por este trabalho possa ser difundido e utilizado na prática, com a expectativa de que proporcione o alcance de suas funcionalidades para quem porventura necessitar da implementação de sua Política de Segurança da Informação.

Ao término deste trabalho, ficam-se sugestões para desenvolvimentos futuros, dentre elas: a proposição de reavaliações evolutivas sobre os tópicos eleitos na Política de Segurança da Informação apresentada, para verificar sua aderência às exigências da Lei Geral de Proteção de Dados depois que se decorra a vigência de sua aplicação mais recorrente e a busca por possíveis adequações ao modelo, para aperfeiçoamento de sua utilização.

REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27002 Tecnologia da informação – Técnicas de segurança – **Código de prática para a gestão de segurança da informação**. ABNT, 2005.

AGÊNCIA SENADO. **Lei Geral de Proteção de Dados entra em vigor**. Disponível em: <https://www12.senado.leg.br/noticias/materias/2020/09/18/lei-geral-de-protecao-de-dados-entra-em-vigor>. Acesso em: 15 de jun. de 2021.

ANPD. **Guia Orientativo Sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte**. v. 1, 2021.

AUDY, J. L. N.; ANDRADE, G. K.; CIDRAL, A. **Fundamentos de Sistemas de Informação.** Porto Alegre: Bookman, 2005.

BASTOS Alberto; CAUBIT, Rosângela. **Gestão de Segurança da Informação.** ISO 27001 e 27002 Uma Visão Prática. Rio Grande do Sul. Zouk, 2009.

BEAL, Adriana. **Segurança da Informação.** Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações. São Paulo. Atlas,2005 – Reimpressão 2008.

BRASIL. **Lei n. 12.965 de 23 de abril de 2014.** Marco Civil da Internet. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 08 de jul. de 2021.

BRASIL. **Lei n. 13.709 de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 26 de mai. de 2021.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Artigo 58-A. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 15 ago. 2018. Disponível em: <https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/39390120/do1-2018-08-15-lei-n-13709-de-14-de-agosto-de-2018-39390064>. Acesso em: 20 jan. 2025.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 (Lei Geral de Proteção de Dados Pessoais -

LGPD). Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 15 ago. 2018. Disponível em: <https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/39390120/do1-2018-08-15-lei-n-13709-de-14-de-agosto-de-2018-39390064>. Acesso em: 20 jan. 2025.

BRASIL. **Lei n. 9.784 de 29 de Janeiro de 1999.** Lei de Procedimento Administrativo. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9784.htm>. Acesso em: 09 de jul. de 2021.

CAETANO, João Victor Lima. **O regulamento geral de proteção de dados (GDPR).** Cadernos Eletrônicos Direito Internacional Sem Fronteiras, v. 2, n. 1, p.e20200111-e20200111, 2020. Disponível em: <https://cedisf.emnuvens.com.br/cedisf/article/view/76>. Acesso em 16 Jul. 2021.

COTS, M., OLIVEIRA, R. **Lei geral de proteção de dados pessoais comentada.** São Paulo: Thomson Reuters Brasil, 2018.

DE MATTOS, Alessandro Nicoli. **Informação é prata, compreensão é ouro:** um guia para todos sobre como produzir e consumir informação na era da compreensão. Alessandro Nicoli de Mattos, 2010.

FERREIRA, A. B. H. **Novo Aurélio - Dicionário da Língua Portuguesa.** São Paulo: Ed. Nova Fronteira, 1999.

FONTES, Edison. Políticas e Normas para segurança da informação**. Como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações**. Rio de Janeiro: BRASPORT, 2012.

FORTES, V. B. **Os direitos de privacidade e a proteção de dados pessoais na internet.** Rio de Janeiro: Lumen Juris, 2016.

HOUAISS, Antônio. **Dicionário Houaiss da Língua Portuguesa.** Rio de Janeiro, Ed. Objetiva, 2001.

LAUDON, K. C. S.; JANE, P. **Sistemas de informações gerenciais**: administrando a empresa digital. SãoPaulo: Prentice Hall, 2004.

LYRA, Maurício Rocha. **Segurança e Auditoria em Sistemas de Informação.** Rio de Janeiro. Ciência Moderna, 2008.

MACHADO, Felipe Nery Rodrigues. **Segurança da informação: princípios e controle de ameaças**. Saraiva Educação SA, 2014.

MARTINELLI, D. P.; VENTURA, C. A. A. **Visão Sistêmica e Administração** – Conceitos, Metodologias e Aplicações; 1º Edição; Editora Saraiva; São Paulo, 2006.

MENEZES, A. J.; OORSCHOT, P. C.; VANSTONE, S. **A. Handbook of applied cryptography**. CRC Press, 1996.

MONTEIRO, Y. S. **A efetividade dos mecanismos de proteção de dados pessoais na Lei 13.709/2018.** Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília, Brasília, 2019. Disponível em: <https://repositorio.uniceub.br/jspui/handle/prefix/13383>. Acesso em: 09 de jul. de 2021.

PIWOWAR, H. A.; DAY, R. S.; FRIDSMA, D. B. **Sharing detailed research data is associated with increased citation rate**. PLoS ONE, v. 2, n. 3, p. e308, 2007. Disponível em: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0000308>. Acesso em: 20 jan. 2025.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**. Uma visão executiva. Rio de Janeiro. Elsevier, 2003 – 11º reimpressão.

SILVA T.P; CARVALHO H; TORRES B.C. **Segurança dos Sistemas de Informação – Gestão Estratégica da Segurança Empresarial**. Portugal. Atlántico, 2003.

SOARES, Sória Pereira Lima; DA SILVA SOARES, Augusto Cezar; ALVES, Aldo Agustinho. **A Importância da Implementação de uma Política de Segurança da Informação**. *Brazilian Journal of Development*, v. 7, n. 4, p. 37162-37171, 2021.

STONER, J. A. F.; FREEMAN, R. E. **Administração.** Rio de Janeiro: Editora LTC, 2000.
WALTERS, J. P.; LIANG, Z.; SHI, W.; CHAUDHARY, V. **Wireless sensor network security**: survey. In XIAO, Y. Security in distributed, grid, mobile and pervasive computing, p. 367-417, 2006.

TENOPIR, C.; ALLARD, S.; DOUGLAS, K. et al. **Data sharing by scientists: practices and perceptions**. PLoS ONE, v. 6, n. 6, p. e21101, 2011. Disponível em: <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0021101>. Acesso em: 20 jan. 2025.

ZHOU, Y.; FANG, Y. **Network security and attack defense**. In ZHENG, J.; JAMALIPOUR, A. Wireless sensor networks: a networking perspective. Wiley, 2009.