XXII ENGEMA
Encontro Internacional sobre Gestão Empresarial e Meio Ambiente

ISSN: 2359-1048
Novembro 2020

IMPLEMENTAÇÃO DE POLÍTICAS DE SEGURANÇA DE INFORMAÇÕES EM EMPRESAS DE ACORDO COM A LEI GERAL DE PROTEÇÃO DE DADOS N°13.709/18 E DESAFIOS PARA A CONTABILIDADE

BRUNA BENITA WEBER SANCHEZ LOPEZ
UFSC UNIVERSIDADE FEDERAL DE SANTA CATARINA

SÉRGIO MURILO PETRI
UNIVERSIDADE FEDERAL DE SANTA CATARINA

IMPLEMENTAÇÃO DE POLÍTICAS DE SEGURANÇA DE INFORMAÇÕES EM EMPRESAS DE ACORDO COM A LEI GERAL DE PROTEÇÃO DE DADOS N°13.709/18 E DESAFIOS PARA A CONTABILIDADE

1.INTRODUÇÃO

Em um mundo altamente conectado com a utilização de tecnologias de informação, a internet está presente em smartphones e computadores, gerando dados com crescimento exponencial, que, de acordo com a previsão da International Data Corporation - IDC (2019) a quantidade de dados criados em 2020 crescerá 44 vezes, atingindo 35 zettabytes.

Diante dessa abundância de dados, empresas tomaram posse dessas informações para mudar a natureza da concorrência. Na coleta dos dados, teriam a disposição um escopo de informações que poderá auxiliar no melhoramento de seus produtos e atrair mais clientes. Para confirmar as evidencias da transformação digital denominado por alguns como "O petróleo da era digital", gigantes de tecnologia como Google, Facebook, Amazon, Apple e Microsoft concentram seu poder no controle de dados como se fossem ativos próprios e as negociam, e, com isso, arrecadam milhões de dólares em lucro (BISSO et. al, 2020).

Com o processamento de dados, as entidades conseguem aumentar sua eficácia quanto a tomada de decisão de forma mais assertiva e rápida, criando assim, uma estrutura personalizada que combina gerenciamento, consultoria e treinamento. Outra vantagem é a verificação de tendências e padrões, por meio de técnicas e estatísticas avançadas da área da ciência de dados, trazendo resultados proativos aos negócios com marketing mais personalizado e fidelização de clientes.

Porém, além das vantagens mencionadas, a circulação e exposição desses dados pelas redes virou alvo de ataques cibernéticos com apropriação por criminosos e crackers. Trata-se também do combate ao "ransomware", palavra em inglês que deriva da mistura de "ransom" (resgate) e "software" (programa de computador) que após inúmeras ataques tornou as instituições em vítimas de sequestros dos bancos de dados, aplicativos e rede, expondo pessoas e promovendo o pagamento por resgastes no mundo todo (SILVA; TEIXEIRA, 2019). Essa ameaça cibernética tem preocupado não apenas empresas e consumidores, mas também governos ao redor do mundo.

De acordo com o Decreto n°10.222/2020, que trata sobre a estratégia Nacional de segurança cibernética, menciona-se que "A digitalização quase total dos modelos de negócios tornou a economia global mais eficiente e dinâmica, e também mais vulnerável a ataques cibernéticos", no entanto, toda essa complexidade das ameaças coloca em risco a confiança no mundo digital, fator imprescindível para as atividades online (BRASIL, 2020).

Ademais, diversas indagações são feitas em relação a delitos virtuais e os pagamentos feitos diante dessas ameaças. O relatório da Sophos "The State of Ransomware 2020" relata que pagar criminosos cibernéticos para restaurar dados criptografados de empresas durante um ataque de ransomware, gerou despesas de 2,55 milhões em 2019 no Brasil (SOPHOS; 2020). Já pesquisas feitas pela empresa de antivírus Eugene Kaspersky, relatou que o cenário de pandemia foi alvo de aumentos de ataques dos cibercriminosos, com a transferência de funcionários para o regime home office, com o bloqueio de mais de 30 mil ataques em todo o mundo, estando o Brasil na liderança desses números (EUGENE KASPERSKY, 2020). Outro estudo relevante, traz referência ao tratamento dos dados, a pesquisa da McAfee, em 2018, demonstrou um aumento de 53% no compartilhamento de dados sensíveis em nuvem em relação a 2017. Ainda evidenciou que 21% de todos os arquivos na nuvem contêm dados confidenciais. Já o levantamento chamado "Smart Protection Network", produzido pela empresa de cibersegurança Trend Micro, estima que 1,8 bilhões de ransomwares foram capturados pela empresa no período de janeiro de 2016 a março de 2019.

Neste ambiente de instabilidade na segurança de dados nas empresas, , o Brasil adotou um regime para a proteção de dados com a lei n°13.709/18, assim como na União Europeia em 2016, que coloca em discussão direitos e proteções a informações pessoais e fornece diretrizes sobre a coleta e o tratamento de dados pessoais de pessoas físicas e jurídicas em posse das empresas a nível nacional, como a sansões cabíveis em caso de descumprimento.

O cenário de ameaças virtuais se mostra cada vez mais frequente para as organizações quanto em escritórios ou departamentos contábeis que agrupam informações, muitas vezes confidenciais, tanto de pessoas jurídicas quanto de pessoas físicas. O mercado contábil é estruturado sobre leis, normas e regulamentações que devem ser obedecidas. Toda essa prática legal serve para demonstrar integridade aos esforços anticorrupção anexadas a programas de compliance. Após 2018, as exigências da lei LGPD deverão ser inclusas nos termos de conformidade dos escritórios contábeis.

Nesse contexto, é desafiador para as empresas buscar meios de prevenção a possíveis ameaças cibernéticas promovendo segurança aos seus dados e informações, por isso, **quais seriam as boas práticas e políticas de segurança de informação a serem adotadas pelas empresas e profissionais de contabilidade nos seus programas de conformidade?**

Para responder ao questionamento, delimitou-se como objetivo desta pesquisa a busca de indicadores para a construção de um compliance digital, com políticas de segurança, de acordo com a nova lei Geral de Proteção de dados n°13.709/18 e as normas de padronização e certificação internacional NBR ABNT ISO 27001 e 27002:2013. Para tanto, se utilizara referências a normas e pesquisas de segurança de dados.

Visto a importância da informação como ativo da organização, este trabalho justifica-se também para a busca de uma maior compreensão sobre a utilização de tecnologias de segurança da informação, com a intenção de fornecer um ambiente seguro para a atuação contábil, visto que o profissional contábil não possui uma percepção mais apurada sobre segurança cibernética, se tornando mais vulnerável para ataques (Herath, 2011).

2.REVISÃO DA LITERATURA

2.1 Lei Geral de Proteção de dados

As empresas tratavam os dados coletados como ativo próprio, que poderiam ser livremente utilizados e comercializados por quem deles se apropriasse (EPEDINO; FRAZÃO; OLIVA, 2019). Nesse panorama, o Estado identificou a necessidade de implantar um programa de proteção de dados, assim como realizado na União Europeia pelo Parlamento Europeu em 2016. Por isso, em 14 de agosto de 2018, foi sancionada a lei n°13.709/18 a chamada LGPD – Lei Geral de Proteção de dados, que fornece diretrizes sobre a coleta e o tratamento de dados pessoais em posse das empresas a nível nacional, até mesmo nos meios digitais, tanto por pessoa natural quanto por pessoa jurídica de direito público ou privado (BRASIL, Art.1, 2018). Atualmente a LGDP está previsto para entrar em vigor a partir de 2020, porém, com a situação emergencial da pandemia do Covid -19, estimasse um prazo de prorrogação. Embora não se tenha o prazo definitivo, as empresas devem estar preparadas para ajustar-se aos comandos da nova legislação.

Monteiro (2018) diz que a LGPD também busca equilibrar interesses econômicos e sociais, restringindo a continuidade de decisões automatizadas e limitando abusos nesse processo, por meio da diminuição da assimetria de informações, e, por consequência, de poder, entre o indivíduo, setor privado e o Estado. Ademais, a LGDP determina que a regulamentação deverá ser respondida por empresa pública e privada, pessoa física e jurídica que, colete, armazene, trate ou manipule dados dos cidadãos, independente da nacionalidade, podendo chegar a multas de 50 milhões de reais em caso de descumprimento (BRASIL, 2018).

No artigo 2º da LGPD, a matéria de proteção de dados diz respeito aos princípios que trazem traços norteadores para auferir maior garantia aos titulares dos dados, proporcionando gerenciamento e utilização para as finalidades pretendidas. Assim, inicialmente, no seu Art. 5°,

efetua a diferenciação entre dados pessoais, dados pessoais sensíveis e dados anonimizados, sendo:

Figura 1 – Tipologia de dados

Dado Pessoal	Dado Pessoal Sensível	Dado anonimizado
• Informação relacionada a pessoa natural identificada ou identificável.	• 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.	• Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Fonte: Elaborado pelos autores com base no Art.5 Lei 13.709/18.

Entende-se como dados pessoais aquela informação relacionada ao nome, sobrenome, endereço, idade, localização, número de IP, histórico de compras, etc. relacionados a pessoa natural viva (PINHEIRO, 2020). Já o dado pessoal sensível é objeto de proteção, tendo em conta o potencial lesivo de sua utilização, por ter característica da personalidade do indivíduo, propiciando possivelmente discriminações abusivas (DEPEDINO; FRAZÃO; OLIVA, 2019). Referente aos dados de anonimização, são aqueles utilizados de meios técnicos razoáveis e disponíveis no momento de tratamento (PINHEIRO, 2020).

No seu Art. 9°, a Lei Geral de Proteção de Dados Pessoais estabelece direitos ao titular para que seja informado sobre o tratamento de seus dados, que deverão ser apresentados de forma clara, adequada e ostensiva, junto as seguintes características:

> I - Finalidade específica do tratamento;
> II - Forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador;
> IV - Informações de contato do controlador; [...]

Além disso, o controlador deverá atender, de forma gratuita, no tocante do art. 18 da LGPD, às solicitações do titular realizadas mediante requerimento a qualquer agente de tratamento com as garantias dos incisos I ao IX, na qual as empresas devem respeitar a confirmação da existência de tratamentos de dados, acesso aos dados tratados, correção, anonimização ou eliminação de dados desnecessários, portabilidade, compartilhamentos e consentimento (BRASIL, 2018).

A LGPD também adota definições quanto aos agentes que farão o tratamento dos dados, que na definição de Pinheiro (2020) existe quando "o controlador recepciona os dados pessoais dos titulares por meio de consentimento e o operador realiza algum tratamento de dados pessoais motivados por contrato ou obrigação legal", abraçadas pelos incisos V ao IX do art. 5.

Quadro 01 – Agentes dos dados

Objeto de tratamento	Definição
Titular	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento
Controlador	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento
Operador	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador
Encarregado	Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)
Agentes de tratamento	O controlador e o operador

Fonte: Elaborado pelos autores com base na Lei 13.709/18.

No tocante do artigo 46 da LGPD, controladores e operadores, na condição de agentes de tratamento, devem adotar medidas de segurança, técnicas e administrativas, capazes de proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas que possam provocar destruição, perda ou qualquer outra forma de tratamento inadequado ou ilícito

(BRASIL, 2018). Tais medidas, relacionadas com o princípio da segurança, visam à proteção da informação de inúmeras ameaças, a fim de assegurar a continuidade do negócio, diminuindo os riscos, com o objetivo de confidencialidade e integridade dos dados. (COTS; OLIVEIRA, 2019).

Se tratando da governança em privacidade, a normativa dispõe no artigo 50, que os controladores e os operadores, de acordo com suas competências, poderão elaborar regras de boas práticas e de governança, devendo conter no mínimo os requisitos do inciso I. Nesse sentido, esse programa é o conjunto de boas práticas a serem adotadas pelos agentes de tratamento de dados, com o objetivo de cumprir ordens legais. Ademais, o art. 50, direciona requisitos a serem observados pelas empresas e realizadas pelos envolvidos como mecanismos de supervisão e mitigação de riscos (BRASIL, 2018).

Em caso de descumprimento às exigências previstas na LGDP, o Art. 52 prevê a aplicabilidade de sansões administrativas, sendo a Autoridade Nacional de Proteção de Dados o órgão competente pela aplicação e fiscalização, com multas de até 2% do faturamento, limitado a 50 milhões de reais (BRASIL, 2018). Assim, qualquer violação à LGPD, as empresas estarão sujeitas a multas e sansões, abrangendo até as matérias menos objetivas, dando ênfase aos agentes de tratamento, ou seja, ao controlador e operador como responsáveis em caso de violação da segurança e pelos danos causados (COTS; OLIVEIRA, 2019).

2.2 Compliance de dados

A sugestão de um programa de governança em privacidade está delineada no artigo 50, a qual propõe um conjunto de regras de boas práticas e governança a serem utilizadas pelos agentes de tratamento de dados pessoais. De acordo com o inciso I, do artigo supracitado, ao implementar o programa de governança em privacidade, deve conter, no mínimo:

Quadro 2 – Programa de governança e princípios

Programa de governança em privacidade Art. 50 Inc. I		
Requisitos mínimos	**Principio**	**Referência legislativa - LGDP**
Demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais	segurança e prevenção	Art. 6º, VII, VIII
Seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta	livre acesso	Art. 6º, IV
Seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados	não discriminação e adequação	Art. 6º, IX, II
Estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade	responsabilização e prestação de contas	Art. 6º, X
Tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular	transparência e Princípio do livre acesso	Art. 6º, VI, IV
Esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos	adequação e Princípio da adequação	Art. 6º, X, II
Conte com planos de resposta a incidentes e remediação	prevenção	Art. 6º, VIII
Seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas	finalidade e Princípio da qualidade dos dados	Art. 6º, I, V

Fonte: Lei LGDP n°13.709/2018.

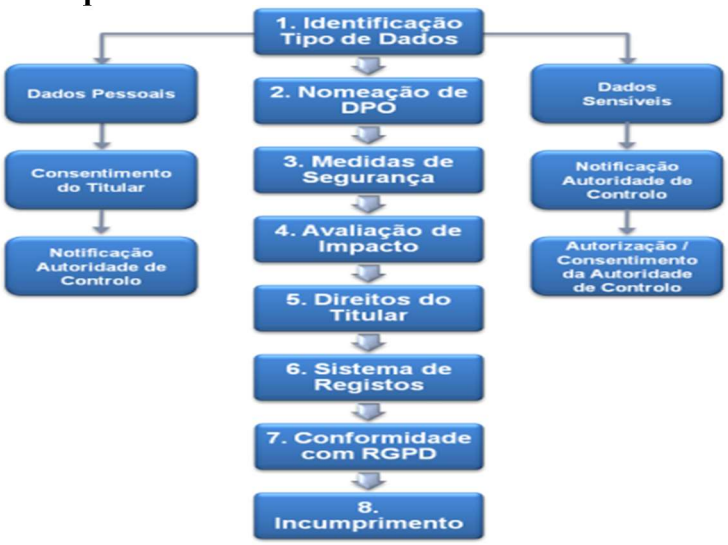
Ao elaborar as regras de boas práticas, os agentes de tratamento precisarão analisar quanto ao tratamento e aos dados "a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados do titular" afim de se assemelhar a política de segurança da informação com objetivo de cumprir ordens legais (BRASIL, 2018). Com isso, o controlador fica responsável também de formular uma estrutura de volume das suas operações, bem como identificar a sensibilidade dos dados e a possibilidade e gravidade dos danos para os titulares dos dados (BRASIL, 2018). Entende-se, portanto, que a LGPD orienta os controladores a inserirem as políticas de governança em privacidade em sua estrutura geral, como mecanismo de conformidade a LGPD, sendo um conjunto de diretrizes de boas práticas, equiparado aos programas de compliance, com o propósito de cumprimento de normas legais, políticas internas e a realização de uma gestão de riscos, (KOEPSEL, 2020). Depedino, Frazão e Oliva (2019) alegam que a adoção de boas práticas de governança de dados, colaborara na construção de uma relação de confiança com o titular dos dados, por meio de atuação transparente, o que pode se tornar um diferencial competitivo nos negócios.

Induz-se por compliance nas palavras de Pfaffenzeller (2015) como o "conjunto de práticas e disciplinas adotadas no intuito de alinhar o seu comportamento coorporativo à observância das normas legais e das políticas governamentais aplicáveis ao setor de atuação, prevenindo e detectando ilícitos". Desse modo, o programa permite estabelecer conformidade que estejam alinhadas às regras da empresa e assim assegurar seu cumprimento, tendo o objetivo de prevenção e minimização de riscos aos quais as empresas estão expostas (SANTOS; AMARAL; SILVA, 2020).

Portanto, visto a importância do programa de conformidade, o compliance de dados pessoais volta-se justamente para auxiliar aos empresários a aplicação de forma efetiva as normas de proteção de dados, afim de minimizar incidentes que impliquem responsabilidade empresarial (BLUM; ZEPERLIM, 2020). Por essa razão, é importante investir em um programa de compliance, com cibersegurança seguro e bem elaborado, são formas de prevenir e resguardar uma empresa da aplicação de sanções dentro do âmbito da LGPD (SANTOS, 2019).

Nesse cenário, se tratando da importância e implementação do programa de compliance da LGPD no ambiente corporativo, De Farias (2018), tenta explicar com um fluxograma, os possíveis passos a serem seguidos para facilitar a sua incorporação nas políticas já existentes de mitigação de riscos.

Figura 2 – Fases do compliance



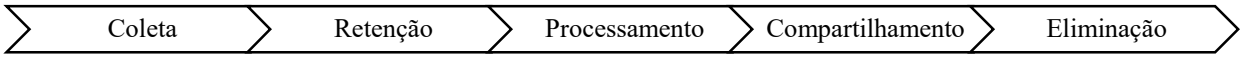
Fonte: De Farias (2018).

Nessa visão, Depedino, Frazão e Oliva (2019) também afirmam que a adequação da conformidade com a LGDP, demandará a inclusão na estruturação de mecanismos direcionados já existentes, a fim de assegurar o cumprimento à legalidade no tratamento de dados pessoais

associados às boas práticas corporativas. É importante, a luz da legislação pertinente, que a entidade seja capaz de adotar procedimentos para as hipóteses de tratamento de dados pessoais, atendendo também, as condições de segurança, confidencialidade e integridade dos dados armazenados (DEPEDINO; FRAZÃO; OLIVA, 2019).

Ao saber os requisitos para a implementação do compliance na empresa, deve-se conhecer o fluxo de vida dos dados gerados para então identificar os riscos inseridos no tratamento dentro da corporação. Para isso, A guia de boas práticas da Lei Geral de proteção de dados, divulgados pelo Governo Federal em abril (2020) menciona que existe coleta quando há obtenção, recepção ou produção de dados pessoais independente do meio utilizado; a retenção quando há armazenamento independente do meio utilizado; processamento quando envolve classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais; compartilhamento quando a operação envolva transmissão, distribuição, comunicação, transferência, difusão e compartilhamento de dados pessoais; e finalmente eliminação quando existe operações que visam apagar ou eliminar os dados qualquer operação que visa apagar ou eliminar dados pessoais (GUIA DE BOAS PRÁTICAS LGDP, 2020).

Figura 3 - Ciclo de vida do tratamento de dados



Fonte: Guia de Boas Práticas - LGDP (2020).

Na visão de Pinheiro (2020) tratamento de dados é "toda operação realizada com algum tipo de manuseio de dados pessoais. Nesse sentido, o Art. 7º, do inciso I ao X, traz preocupações sobre quando poderá ser realizado o tratamento de dados, como mediante consentimento do titular, obrigação legal e para realização de estudos por órgão de pesquisa.

Apresentado os problemas envolvendo a coleta, o uso, o tratamento e o destino de dados e o direito à privacidade, as entidades, sejam públicas ou privadas, terão que se adaptar às novas regras previstas na LGDP (SANTOS, 2019), com a revisão e atualização das cláusulas de contratos com parceiros que exercem alguma operação com dados, como também, na transparência em sites corporativos sobre as políticas de privacidade adotadas (KOEPSEL 2020).

2.4 Ataques cibernéticos em ambientes corporativos

De acordo com Wentd e Jorge (2013) o termo "crimes cibernéticos" pode ser usado para definir delitos praticados por intermédio de computadores ou dispositivos moveis de forma ilegal ou sem autorização. Nesse sentido, o Relatório Nacional digital no Brasil (2018) alega que poderá existir atividade ilícita por cibercrimes realizados pela internet ou dispositivo eletrônico, se este se encontrar vulnerável. Entende-se por vulnerabilidade, como falha ou erro de software ou sistema, permitindo ataques de hackers com propósitos maliciosos, sendo o hacker aquele que acessa aos dispositivos, software ou rede com conhecimento avançado em computação (PSAFE, 2018).

O número de ataques tem crescido no Brasil desde 2001, colocando como alvos todos os setores, incluindo a agencias e entidades públicas, organismos internacionais e partidos políticos, devido a fragilidade na defesa cibernética encontrada pelo hacktivismo (LIMA, 2018). A seguir no quadro 3, Bisso et. al, (2020) mostra um panorama das multas aplicadas a algumas empresas conhecidas:

Quadro 3 – Penalidades aplicadas a empresas

Valor	Empresa	País	Ano
US$ 4 B	Facebook	EUA	2019
£ 183,39 M	Britinish Arways	Reino Unido	2019
US$ 148 B	Uber	EUA	2018
US$ 85 M	Yahoo	EUA/Israel	2018

€ 50 M	Google	França	2019
US$ 22,5 M	Google	EUA	2012
US$ 10 M	Blue Cross Blue Shield	EUA	2019
US$ 3,8 M	AMCA	EUA	2019
R$ 1,5 M	Banco Inter	Brasil	2018
€ 600 M	Uber	Holanda	2018
£ 385 M	Uber	Reino Unido	2018

Fonte: Bisso et. al, (2020).

Os dados dessa pesquisa demonstram que muitas empresas de grande porte, apesar das suas estruturas fortes no mercado, precisam considerar a segurança cibernética como ação prioritária de investimentos, elaborar planos de gestão de riscos e de tratamento e resposta a incidentes, assim como planejar orçamento adequado para combater os incidentes de segurança (BISSO, et. al, 2020).

Diante desse aumento de investida, Custoias e Mendonça (2019) reconhecem que a utilização de sistemas antigos por muitas instituições pode ser a causa dos ataques, os quais os deixa vulneráveis, permitindo a não resistência a ciberataques com consequências de perdas financeiras milionárias, custos indiretos e danos à imagem (CUSTOIAS; MENDONÇA, 2019). Nesse sentido, Conte (2018) pede ênfase a problemas relacionados a cybersecurity, já que usuários e funcionários nas empresas cometem erros devido às poucas habilidades em segurança cibernética, e acabam acessando links e executando arquivos maliciosos sem saber do perigo que está por trás, o que representa cerca de 72% a 95% das ameaças de segurança cibernética nas organizações. Assim, os cibercriminosos apostam em dois fatores para aplicar golpes: vulnerabilidade nos sistemas de segurança corporativa e a falta de treinamento dos funcionários.

As ameaças cibernéticas têm o escopo de alcançar grande número de organizações por prestarem serviços essenciais à sociedade, possuem elevado nível de criticidade. Por isso, essas organizações necessitam de meios de gerenciar os riscos das ameaças cibernéticas, e de ferramentas de automação de segurança que usam inteligência artificial e aprendizado de máquina, que permitam analisar, identificar e conter os ataques cibernéticos (BRASIL, decreto n°10.222/2020).

Nesse contexto, visualiza-se que os ataques cibernéticos, caso não sejam adequadamente tratados, podem afetar profundamente a reputação da organização, ocasionar perda de receitas, levar a prejuízos operacionais com a paralização dos serviços, resultar em perda de informações e ainda levar à aplicação de sanções legais e administrativas (BRASIL, decreto n°10.222/2020). Ademais, existe um rol de exemplos de ameaças e vulnerabilidades descritas nos anexos C e D da ISO 27005:2019 que podem nortear e facilitar a identificação, assim como a disponibilização de ameaças em tempo real no site da Center for Internet Security – CIS25.

2.4 Segurança dos dados ou cibersegurança no ambiente contábil

Normalmente os usuários finais de computadores são os elos mais fracos da cadeia de segurança cibernética devido a suas habilidades limitadas de evitar danos a TI através da internet, que muitas vezes são sanadas com pesquisas feitas de forma autônoma (CUSTOIAS; MENDONÇA; CUNHA, 2019). Assim, os autores manifestam a necessidade de ter uma "estrutura de avaliação rápida baseada em critérios de segurança bem estabelecidos que permitam às organizações detectar falhas de segurança tão rapidamente quanto as ameaças", vindo a solucionar essas vulnerabilidades antes das invasões (CUSTOIAS; MENDONÇA; CUNHA, 2019).

Se tratando de debates sobre segurança no espaço cibernético, o decreto n°9.637/2018 traz a definição de segurança da informação como "área sistêmica e diretamente relacionada à proteção de um conjunto de informações e ao valor que estas possuem para um indivíduo ou para uma organização". Desse modo, a segurança da informação abrange a segurança

cibernética, a defesa cibernética, a segurança física e a proteção de dados organizacionais (BRASIL, 2018).

2.4.1 Segurança de dados, controles gerenciais e auditoria

Amir et., al (2018) afirma que os ataques cibernéticos são um dos principais riscos que as entidades devem controlar. Nessa linha, Haapamaki e Sihvonen (2019) traz visões sobre a inclusão da consciência de ameaça cibernéticas na gestão das empresas e no investimento em tecnologia de segurança, também influenciados pela regulamentação, se tornando parte de um controle gerencial o sistema de cibersegurança. Assim, na visão gerencial, os objetivos da segurança cibernética podem ser divididos em três categorias amplas: primeiro, cibersegurança protege a confidencialidade das informações privadas; em segundo lugar, garante que os usuários autorizados podem acessar as informações em tempo hábil e, terceiro, a segurança cibernética protege a precisão, confiabilidade e validade da informação (HAAPAMAKI; SIHVONEN, 2019).

Ganser e Lucysgyn (2005) refletem sobre as vulnerabilidades às ameaças cibernéticas em empresas públicas e privadas pela sua plena dependência às tecnologias da informação e redes para o funcionamento de seus sistemas de gestão financeiros. Somado a essa preocupação, contadores e gerentes, a qual trabalham com economia, que é baseada em conhecimento, devem se preocupar em proteger seus ativos de informação (GORDON et. al, 2008). Nesse sentido, cabe ao profissional contábil ter conhecimento quanto ao momento em que deve agir e as ferramentas que pode adotar para auxiliar na proteção, para isso, o primeiro passo é desenvolver um conjunto de políticas de segurança da informação (Knapp, Marshall, Byrd & Morris, 2009).

Haapamaki e Sihvonen (2019) entendem que a segurança cibernética se tornou extremamente importante para a contabilidade e políticas públicas, devido à grande bagagem de informações que possuem sobre as organizações. Nessa linha, a cibersegurança pode ser considerada como parte do controle da contabilidade gerencial e assunto alinhado a auditoria, sujeito a análise de custo-benefício, avaliação de controle interno e considerações de política de divulgação (HAAPAKI; SIHVONI, 2019).

Alinhado a área de auditoria, Stafford et al. (2018, p. 420) argumentou que "o auditor é provavelmente o consultor objetivo mais valioso e crítico do processo que é projetado para gerenciar e fazer cumprir a conformidade de segurança na empresa", sendo a empresa responsável por adotar a orientação da auditoria em matéria de melhoria cibernética. Pathak (2005) destaca que os auditores devem estar informados sobre a gestão de riscos em tecnologia, para medir o seu impacto nos controles internos e vulnerabilidades organizacionais, trazendo mais certeza nas informações financeiras analisadas.

Nesse seguimento, Islam et. al, (2018) pronuncia que a auditoria pode acrescentar ao processo, sugestões de práticas de segurança, visando apoiar a proteção da integridade de ativos, confidencialidade dos dados, acesso e disponibilidade, sendo de suma importância para as empresas na condução dos seus negócios, criando uma vantagem competitiva para alcançar o sucesso. Se tratando de auditoria interna, recomendações da Comitee of Sponsoring Organizations "O COSO", entidade dedicada à melhoria dos relatórios financeiros, através da ética e efetividade dos controles internos e governança corporativa, traz recomendações que poderiam ser aplicáveis a minimização dos riscos cibernéticos promovendo a resolução à aderência das políticas de compliance. Assim, na esfera de governança em segurança de dados, que busca transparência e confiabilidade, poderia se abraçar as metodologias de controles internos (COSO, 2019).

3. PROCEDIMENTOS METODOLÓGICOS

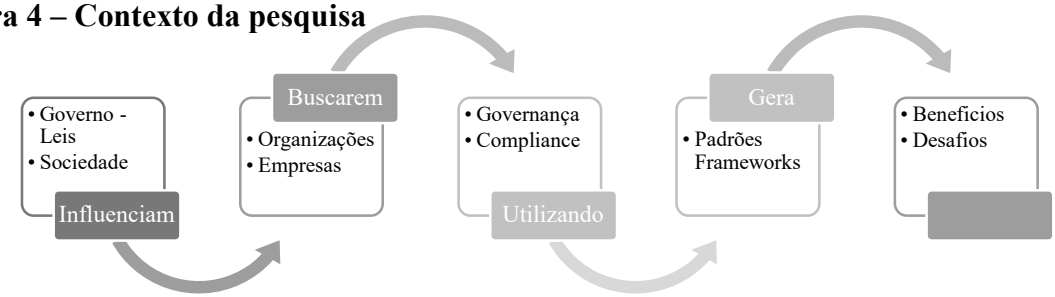
Esta pesquisa se propõe a realizar um estudo sobre segurança cibernética nas empresas, afim de auxiliar na governança, com políticas de proteção de dados, que abrange classificações, diretrizes, etapas, itens relevantes, procedimento de tratamento, de acordo com a nova Lei Geral de Proteção de Dados n° 13.709/18 e as diretrizes da ABNT NBR ISO/IEC 27002: 2013, NBR

ISO/IEC 27001: 2013. Quanto aos objetivos, utilizou-se a pesquisa exploratória, que busca proporcionar maior familiaridade com o problema para torna-lo mais explícito ou construir hipóteses (GIL, 2009). Com relação aos procedimentos, foi aplicada a análise documental, que é constituída de materiais que ainda não receberam um tratamento analítico ou que podem ser reexaminados com vistas a uma interpretação nova ou complementar (NEVES, 1996).

No que diz respeito a abordagem, o estudo teve caráter qualitativo, por aplicar a profundidade dos dados, que na definição de Malhotra (2004) a "pesquisa qualitativa é uma metodologia de pesquisa não estruturada, exploratória, baseada em pequenas amostras, que proporciona insights e compreensão do contexto do problema".

A estrutura de pesquisa deste trabalho se inicia com as seguintes etapas: a) Interpretação da lei n°13.709/2018; b)Compliance de dados; c)Ataques cibernéticos; d)Importância da segurança de dados nas empresas e para os contadores; e)Propostas de políticas de governança para implementação no compliance de acordo a LGDP 13.709/2018 e ABNT NBR ISO/IEC 27001 e 27002.

Figura 4 – Contexto da pesquisa



Fonte: Elaborado pelos autores

4. RESULTADOS

Para análise dos resultados, estabeleceu-se métricas e indicadores que auxiliem projetos voltados para o compliance em segurança cibernética e permitam o monitoramento das ações referentes a essa área. Assim, serão propostos políticas a serem implementadas nas empresas para orientar, conforme legislação e norma vigentes.

4.1 Sistemas de Gestão de segurança das informações

Pensando em uma estrutura de gestão a ser implementada no compliance e na construção de indicadores de melhorias em matéria de segurança das informações, elaborou-se um sistema de gestão de segurança, ilustrada na figura 7. Na ABNT NBR ISO 27001:2013 é indicado o modelo PDCA "Plan-Do-Check-Act", que compõe um conjunto de ações da SGSI. Porém, verificou-se a necessidade de fazer a avaliação antes do planejamento, a fim de verificar a real situação e vulnerabilidades encontradas na organização e dos ativos que seriam importantes proteger.

Figura 5 – Etapas de compliance de dados

Fonte: Elaborado pelos autores (2020).

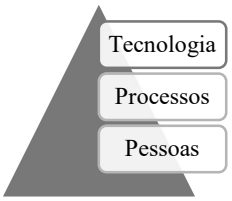
Depois da avaliação, será feito o planejamento, com base nos inventários levantados na primeira fase, nesta etapa se fara a identificação da legislação pertinente e os procedimentos a

serem adotados para seu cumprimento. Visto isso, recomenda-se a adoção de controles e boas práticas para a manutenção das políticas adotadas. Em seguida, se faz necessário a divulgação e treinamento para conscientizar os funcionários sobre as ameaças e obrigações quanto aos operadores, tratamento de dados e informações gerados na empresa.

4.2 Avaliação

Nesta parte do sistema se dará início a avaliação da empresa, com a análise ou auditoria dos ativos que possuem, os riscos e vulnerabilidades a que está submetida. Para tanto, a entidade deverá fazer um levantamento sobre o tratamento relacionado à proteção, inventario e propriedade dos ativos, podendo ser eles a base de dados, documentos, sistemas, unidades organizacionais, locais físicos, equipamentos, entre outros ativos descritos na B.1.3 ABNT NBR ISO 27005:2019, seguindo a hierarquia da figura a seguir:

Figura 6 – Gestão de riscos



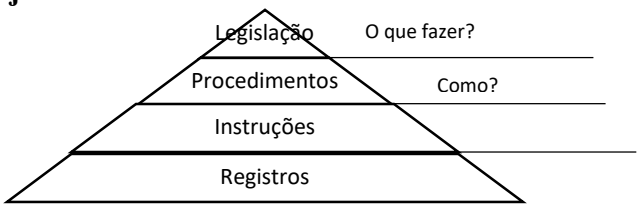
Fonte: ABNT NBR ISO 27002:2013

Dentre as questões que devem influenciar durante a avaliação estão as ameaças e vulnerabilidades, os impactos e a concretização dessas ameaças, a determinação dos riscos potenciais com mensuração dos danos causados. É recomendável classificar os riscos por nível de importância, grau de severidade das perdas e os custos envolvidos. No caso em que o custo da prevenção for maior que seu dano potencial, deve-se tomar outras medidas, as decisões devem ser baseadas na importância do ativo a ser protegido e na continuidade dos negócios.

4.3 Política de segurança e fases do planejamento

A fim de iniciar a política de segurança, definiu-se 4 fases, de acordo com a figura 7.

Figura 7 – Fases do planejamento



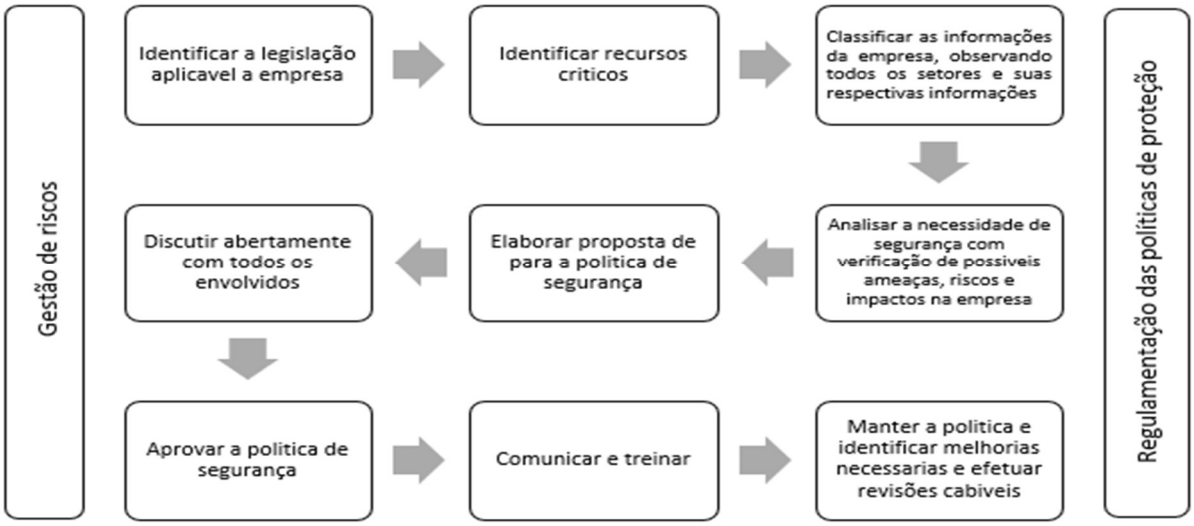
Fonte: Coelho, Araujo, Bezzera (2014).

Conforme a pirâmide, as entidades poderão nortear diretrizes gerais que servirão como politicas, com base nas normas, procedimentos e instruções “o que fazer”. Em uma primeira instancia, será necessário conhecer a legislação em que a empresa é obrigada a seguir e os requisitos necessários para atender que servirão para delimitar as políticas. Em seguida, os procedimentos devem ser implementados nas políticas com controles definidos por padrões e frameworks, respondem ao questionamento “como” a fase do planejamento. Já as instruções, são os detalhes, descrições de um conjunto de operações para a execução da segurança da informação e na identificação dos controles necessários apontados pela análise de risco. Por último, as evidências feitas com o registro dos conjuntos de medidas adotadas para gerar as políticas, com o intuito de permitir a comprovação e impor cumprimento.

4.3.1 Etapas para implementação das políticas de proteção de dados

Nesta sessão serão apresentadas as etapas a serem seguidas para a construção das políticas de proteção de dados de acordo com a ABNT NBR ISO 27002:2013, como descrita na figura 8 a seguir:

Figura 8 – Etapas para implementação de políticas de segurança de informações



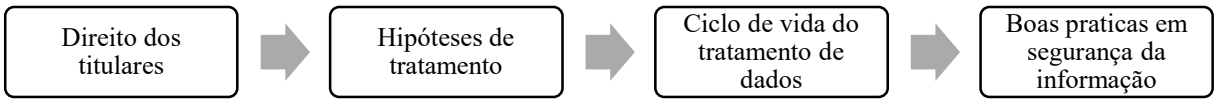
Fonte: ABNT NBR ISO/IEC 27002: 2013.

Como demonstrado, a figura 10 descreve as etapas a serem seguidas para implementação das políticas dentro da organização de acordo com a norma ABNT NBR ISO 27002:2013. Assim, é importante fazer o levantamento de toda a legislação pertinente às informações que a empresa se envolve, para que as políticas não venham a atentar a algumas delas. Na identificação de recursos críticos será abordada aqueles ativos que correm riscos de segurança como Hardware, software, dados em processamento, documentação e suprimentos. A política deve ser documentada e aprovada pelos dirigentes para que possa ser divulgado a todos os envolvidos.

4.4 Gestão da proteção de dados de acordo com a LGDP

Durante a implementação das políticas de segurança da informação na empresa, deverá observar-se a lei geral de proteção de dados, e, sua gestão é importante para atender a legislação e demonstrar comprometimento e proteção aos seus clientes e colaboradores.

Figura 9 – Etapas para a gestão de proteção de dados de acordo com a LGDP



Fonte: Guia de boas práticas LGDP (2020).

4.4.1 Direito aos titulares

A nova estrutura legal atribui aos titulares dos dados pessoais direitos a serem exercidos pelos agentes de tratamento durante toda a existência da posse dos dados. Esses direitos estão relacionados aos princípios estabelecidos a partir do art. 6° da LGDP, do inciso I até o X, além dos específicos, tendo como referência aos arts. 7§I, 8§, 9§, 10§, 11§, 13§, 15§ 16§.

4.4.2 Hipóteses de tratamento

A LGDP autoriza as organizações e entidades a fazerem o tratamento de dados, a serem realizados desde que enquadrados nas hipóteses elencadas na normativa. Para isso, organizou-se um checklist com base na legislação pertinente, descrita na tabela a seguir:

Quadro 4 – Checklist de tratamento de dados

Hipóteses de tratamento	Normas - LGDP
Identificação das hipóteses de tratamento aplicáveis	Art. 7 incisos I ao X
Verificação de conformidade do tratamento quanto aos princípios da LGDP	Art. 6
Especificidades quanto ao tratamento de dados sensíveis	Art. 11

Especificidades para o tratamento de crianças e adolescentes	Art. 14
COLETA	Art. 5 inciso X
ANONIMIZAÇÃO E PSEUDOMINIZÇÃO	
RELATORIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS	Art. 5 e Art. 38
TÉRMINO DO TRATAMENTO	Art. 15

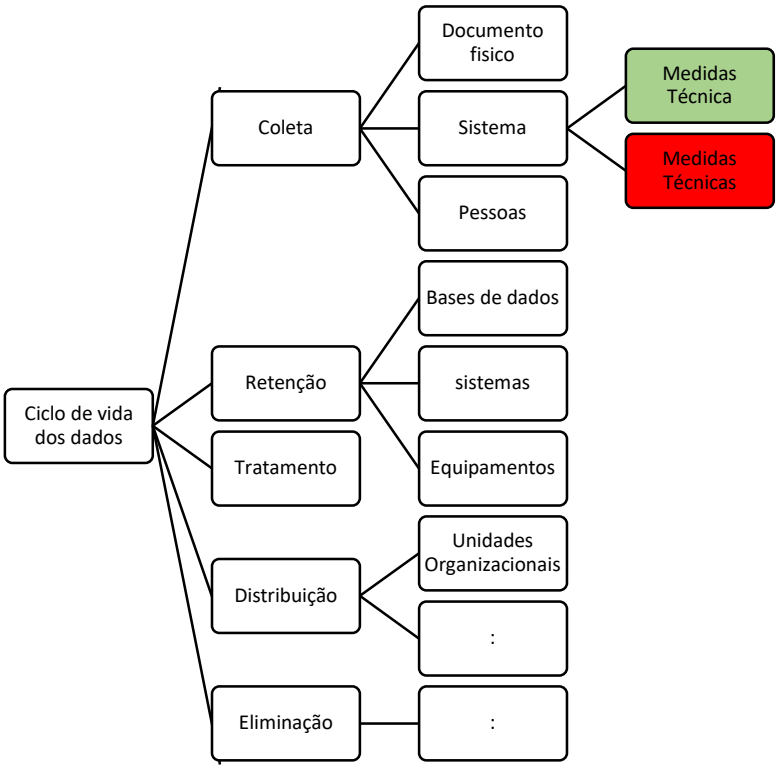
Fonte: Lei n° 13.709/2018

Com a checklist, será possível verificar de forma mais sintética e resumida os principais pontos a serem discutidos sobre tratamento de dados. Em um primer momento, se utilizara da normativa da LGDP n° 13.709/2018, o art. 7, para a identificação das hipóteses de tratamento aplicáveis a serem utilizados pelos operadores, nesses casos, a aplicação dependerá das finalidades e dos contextos específicos de cada situação. Uma vez identificadas as hipóteses de tratamento aplicáveis, deve-se verificar a conformidade quanto aos princípios da LGDP. O art. 5 da legislação em questão, traz especificidades quanto ao consentimento e hipóteses que dispensam consentimento dos dados sensíveis, assim como art. 14 que traz um tratamento de dados sobre crianças e adolescentes. A coleta, trata da operação inicial representado no ciclo de vida dos dados e o art. 5 tenta orientar aos cuidados que devem ser adotados para assegurar sua limitação. Em casos em que o titular deixe de ser anonimado, ou seja, possa então ser identificado, passa a ser considerado pseudomizado, e deverá seguir processos com aplicação de meios técnicos e disponíveis na ocasião do tratamento, de acordo com a LGDP. Se tratando do relatório de impacto à proteção de dados, é um documento que demonstra os processos dos dados coletados, tratados e usados e compartilhados e quais medidas são adotadas para a minimização dos riscos que possam afetar os direito dos titulares podendo ser requisitada pelo órgão fiscalizador (BRASIL, 2018). E por último, o término do tratamento se dá por meio das hipóteses citadas no art. 15.

4.4.3 Ciclo de vida do tratamento de dados

Nesta sessão, será abordada as medidas de segurança a serem implementadas ou ainda não implementadas, de acordo com o mapeamento dos ativos identificados na fase de avaliação.

Figura 10 – Fases do tratamento x Ativos x Medidas de segurança



Fonte: Guia de boas práticas LGDP (2020).

De acordo com as fases do ciclo de vida dos dados que estão presentes nos ativos disponíveis e verificáveis na organização, será necessário a análise e verificação para identificar quais medidas técnicas devem ser adotadas na implementação desses ativos. Para isso, recomenda-se a utilização de frameworks, boas práticas ou normas aplicáveis (GUIA DE BOAS PRÁTICAS LGDP, 2020).

4.3 Boas Práticas em segurança da informação

Dando seguimento ao sistema proposto, no contexto mais amplo de governança, muitos autores e normativas como o decreto n°10.222/2020, entendendo que a legislação não é exaustiva, recomendam a observância a normas e padrões de segurança de informações como Organização Internacional para Padronização (ISO, do inglês International Organization for Standardization), além de outros padrões metodológicos, tais como descritos a seguir no quadro 5:

Quadro 5 – Padrões Frameworks e Controles de segurança cibernética

COBITs	O Control Objectives for information Tecnologies É um framework em governança em TI e apresenta boas praticas para o controle de requisitos, mapas de auditoria, questoes tecnicas e riscos de negocio
ITL	O Information Technology Infraestructure Library é uma biblioteca de boas práticas para gestão de TI de dominio Publico, focando o cliente e a qualidade do serviços de TI, estabelecendo um conjunto de processos gerenciais.
ABNT NBR ISO/IEC 27001:2013.	Sistemas de gestão da segurança da informação
ABNT NBR ISO/IEC 27002: 2013.	Código de Prática para controles de segurança da informação
ABNT NBR ISO/IEC 27005:2019.	Gestão de riscos de segurança da informação
ABNT NBR ISO/IEC 31000:2018.	Gestão de riscos - Diretrizes
ABNT NBR ISO/IEC 27701:2019.	Técnicas de segurança — Extensão da ABNT NBR ISO/ IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes
ABNT NBR ISO 29134: 2017	Provê diretrizes sobre a avaliação do impacto à privacidade.
ABNT NBR ISO 29151:2017	Fornece um guia para os Controladores de dados privados
Center for Internet Security – CIS25	Organização de segurança na internet que identificar, desenvolver, validar, promover e manter soluções de práticas recomendadas para a defesa cibernética.
ABNT NBR ISSO/IEC 27018:2014	Organização de segurança na internet que identificar, desenvolver, validar, promover e manter soluções de práticas recomendadas para a defesa cibernética.
Service Organization Controls (SOC)	Service Organization Controls (SOC)

Fonte: Elaborado pelos autores de acordo com as definições das normativas citadas.

Assim, empresas podem adotar medidas customizadas de segurança e ferramentas, por serem consideradas normas mais evidenciadas para uma boa implementação no contexto de segurança da informação, para tratar riscos de acordo com o modelo de negócio, com a finalidade de melhorar o gerenciamento de vulnerabilidades com condutas, recomendações, princípios e práticas recomendadas, e assim, assegurar a segurança cibernética de possíveis ameaças.

Ademais, o caput do art. 46 da LGPD, instrui que a proteção dos dados pessoais deve ser alcançada com segurança da informação “Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito”(BRASIL, 2018).

4.3.1 Itens relevantes para segurança da informação

Considerando a importância da implementação da LGDP com padrões e controles frameworks como medidas de boas práticas, elaborou-se um quadro comparativo com os principais itens de cada normativa, a fim de fazer uma comparação. Para tanto, utilizou-se como base a ABNT NBR ISO 27001:2013, por ser considerado o mais abrangente em matéria de gestão de segurança de informações e práticas com a implementação e gerenciamento de controles.

Quadro 6- Itens relevantes LGDP X ABNT NBR ISO/IEC 27001:2013 X Tecnologia

	Legal LGDP	**Processos Norma ABNT NBR ISO/IEC 270001:2013**	**Tecnologia**
Política da segurança da informação	*	*	*
Segurança organizacional		*	
Gestão de ativos		*	
Segurança de recursos humanos		*	*
Segurança física e de ambiente		*	
Gerenciamento de operações e comunicações		*	
Controle de acesso	*	*	*
Gestão de incidentes de segurança		*	
Gestão de continuidade do negócio		*	
Conformidade de boas práticas	*	*	
Acessos não autorizados	*	*	*
Situações acidentais	*	*	
Situações ilícitas de destruição, perda, alteração e comunicação ou difusão	*	*	
medidas de prevenção a ocorrência de danos aos dados tratados		*	
Gestão de contratos com terceiros	*		
Propriedade intelectual	*		
Proteção de registros organizacionais	*	*	*
Proteção de dados e privacidade de informações pessoais	*	*	*
prevenção de mau uso de recursos de processamento das informações		*	*
Transparência	*		
Relatório de impacto a proteção de dados	*	*	
Sistemas atualizados		*	*
Proteção contra malwares		*	*
Registros e monitoramentos		*	
Equipamentos		*	
Criptografia		*	*
Responsabilidades dos usuários	*	*	
Tratamento das mídias classificação das informações		*	
Aquisição, desenvolvimento e manutenção de sistemas		*	*
Conscientização, educação e treinamento em segurança da informação e dados pessoais		*	

Fonte: Elaborado pelos autores com base na ABNT NBR ISO 27002:2013; ABNT NBR ISO 27001:2013 e LGDP n° 13.709/2018.

No quadro 6 verificou-se que a norma ABNT NBR ISO 27002:2013 abrange aos principais itens julgados importantes para adaptação às legalidades da LGDP, ademais, deve-se salientar a moldagem à nova norma ABNT NBR ISO 27701:2019 que é uma extensão das normas ABNT NBR ISO 27001 e 27002:2013 com requisitos mais específicos em matéria de privacidade de informações. Além disso, em alguns casos, é imprescindível abraçar essas mudanças com o auxílio da tecnologia.

5. CONCLUSÃO

Diante do exposto, entende-se que segurança das informações engloba segurança de dados pessoais e que o risco de incumprimento ao LGDP pode ser reduzido com a

implementação de um programa de compliance adequado às necessidades e características da empresa, podendo conter políticas de proteção de dados, implementação de controles e boas práticas da ABNT NBR ISOs. Nesse sentido, verifica-se a importância na inclusão de programas de segurança cibernética nas organizações, com uso de modelos reconhecidos que identifiquem a vulnerabilidades, ameaças e riscos, proporcionem diagnósticos e adotem proteções e mecanismos de detecção de ataques e respostas a incidentes.

Mesmo que a lei Geral de proteção de dados n°13.709/2018 não esteja vigente, mostra-se necessário a adequação das empresas na adoção de medidas de proteção, visto que a obtenção e vendas de dados é ilegal e atenta contra os direitos a privacidade e ao livre desenvolvimento da personalidade como previstas no LGDP.

No entanto, entende-se que a certificação e soluções de segurança cibernética é uma meta a ser atingida, devendo considerar a complexidade dos equipamentos, elevado grau de especialização e sistemas de estruturação para conduzir. Quanto aos custos destas medidas, deve existir uma relação entre o nível de segurança e o valor do ativo que se pretende proteger, sendo que o custo não pode ultrapassar o valor do ativo que se pretende proteger. A execução de um programa de compliance voltado às disposições da Lei Geral de Proteção de Dados exige no início uma equipe multidisciplinar, além de investimentos na área, para viabilizar a privacidade dos dados armazenados fisicamente ou digitalmente.

Este artigo, atingiu o objetivo de orientação na construção de políticas de segurança com base na LGDP n° 13.709/2018 e normas de certificado internacional como as ISOS 27001 e 27002:2013 a serem implementadas no compliance, assim como estimular pesquisas de cibersergurança entre acadêmicos e profissionais da contabilidade, visto que, no ambiente administrativo, tem-se acesso a informações financeiras confidenciais, que na falta de conscientização por parte dos funcionários, podem acabar em mãos de criminosos virtuais se não forem instruídos e orientados sobre os perigos da revolução digital. Com isso, se cria uma cultura de respeito à proteção de dados. Além do mais, se tratando de atendimento legal, o requisito do art. 46 da LGDP, que obriga as empresas a atenderem a medidas de segurança técnicas e administrativas, inclui nesse rol da área administrativa à contabilidade.

Dessa forma, concluiu-se que é importante que as organizações públicas ou privadas, estabeleçam políticas e procedimentos de segurança cibernética, iniciando a avaliação dos seus ativos assim como sua importância, adotando o planejamento, com a inclusão de políticas de segurança de proteção de dados, dando ênfase aos direitos abrigados pela LGDP aos titulares dos dados, as hipóteses de tratamento, ao ciclo de vida dos dados e as conformidades e boas práticas com a adoção de normas de certificação internacionais ou frameworks. Por conseguinte, a revisão periódica com o aperfeiçoamento dos processos adotados com programas de capacitação e treinamento contínua aos colaboradores.

Referencias

ABNT NBR ISO/IEC 27001. Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação – Requisitos, 2013.

ABNT NBR ISO/IEC 27002. Tecnologia da informação - Técnicas de segurança - Código de práticas para controles de segurança da informação, 2013.

AMIR, Eli; LEVI, Shai; LIVNE, Tsafrir. Do firms underreport information on cyber-attacks? Evidence from capital markets. Review of Accounting Studies, v. 23, n. 3, p. 1177-1206, 2018.

BLUM, Renato Opice; ZAMPERLIN, Emelyn (ed.). Compliance, responsabilidade empresarial e segurança dainformação.2020.Disponívelem:https://www.lex.com.br/doutrina_27159943_COMPLIANCE_RESPONSABILIDADE_EMPRESARIAL_E_SEGURANCA_DA_INFORMACAO. Acesso em: 15 ago. 2020.

BISSO, Rodrigo et al. Vazamentos de Dados: Histórico, Impacto Socioeconômico e as Novas Leis de Proteção de Dados. Revista Eletrônica Argentina-Brasil de Tecnologias da Informação e da Comunicação, v. 3, n. 1, 2020.

BRASIL. **Decreto n°10.222, de 05 de fevereiro de 2020**. Estratégia Nacional de segurança Cibernética. Brasilia, DF: Presidente da República, 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020-241828419. Acesso em 24 ago 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015- 2018/2018/Lei/L13709.htm. Acesso em: 10 maio 2020

BRASIL. **Decreto 9.637, 26 dezembro de 2018**. Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação. Brasília, DF: Presidente da República, 2018. Disponível: Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação. Acesso em 24 ago 2020.
CONTE, Thomas M. et al. Rebooting Computers to Avoid Meltdown and Spectre. IEEE Computer Society, 2018.
COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais Comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 198.
COSO, Committee of Sponsoring Organizations of the Treadway Commission. Managing Cyber Risk in a digital age. 2019. Disponível em: https://www.coso.org/Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf. Acesso em 15 set 2020.
CUSTOIAS, Gustavo Boldrini; MENDONÇA, Letícia Breda; CUNHA, Daniela Vieira. Estudo sobre solução tecnológica para a mitigação dos riscos cibernéticos no setor financeiro. 2019.
DA SILVA, Felipe Rangel; TEIXEIRA, Rodrigo Valente Giublin. A Sociedade da Informação e seus desafios: a necessidade de efetivação de uma Política Pública de combate ao ransomware no Brasil. RFD-Revista da Faculdade de Direito da UERJ, n. 36, p. 23-52, 2019.
DE FARIA, Cláudia Maria Félix Leite. Gestão da Cibersegurança em empresas Transnacionais relacionadas com Transações Financeiras Críticas de espectro Macroeconómico. 2018.
DEPEDINO, Gustavo; FRAZÃO, Ana.; OLIVA, Milena Donato. Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. São Paulo:Thomson Reuters Brasil, 2019.
DOS SANTOS, Tamires Quintino; DE ARAÚJO AMARAL, Emília; DA SILVA, Fernando Linhares. Compliance: um estudo de caso da empresa Odebrecht. hígia-Revista de Ciências da Saúde e Sociais Aplicadas do Oeste Baiano, v. 4, n. 2, 2019.
EUGENE KASPERSKY. Brasil é líder em empresas atacadas por ransomware na pandemia. Disponível em: https://www.kaspersky.com.br/about/team/eugene-kaspersky. Acesso em 12 jul 2020.
Gansler, J. e Lucyshyn, W. (2005), "Melhorando a segurança dos sistemas de gestão financeira: o queque devemos fazer? ", Journal of Accounting and Public Policy , vol. 24 No. 1, pp. 1-9.
GIL, A. C. Como elaborar projetos de pesquisa. 4. ed. São Paulo: Atlas, p. 175, 2009.
Governo Federal. Guia de Boas Práticas Lei Geral de Proteção de Dados. Abr, 2020, 65p. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 08 ago 2020.
GORDON, Lawrence A. et al. Empirical evidence on the determinants of cybersecurity investments in private sector firms. Journal of Information Security, v. 9, n. 2, p. 133-153, 2018.
HAAPAMÄKI, Elina; SIHVONEN, Jukka. Cybersecurity in accounting research. Managerial Auditing Journal, 2019.

HERATH, Hemantha SB. Cybersecurity: an emerging area for collaborative post-modern management accounting research. Cost Management, v. 25, n. 1, p. 14, 2011.
(IDC), Da International Data Corporation. **Dados**. 2019. Disponível em: https://www.idc.com/. Acesso em: 24 ago. 2020.
ISLAM, Md Shariful; FARAH, Nusrat; STAFFORD, Thomas F. Factors associated with security/cybersecurity audit by internal audit function. Managerial Auditing Journal, v.33, n.4, p. 377-409, 2018.
KNAPP, Kenneth J. et al. Information security policy: An organizational-level process model. Computers & security, v. 28, n. 7, p. 493-508, 2009.
KOEPSEL, Alice de Medeiros. Adoção e efeitos dos programas de compliance à luz da Lei Geral de Proteção de Dados Pessoais. Direito-Tubarão, 2020.
LIMA, Victor Hugo. Hacktivismo e a Defesa Cibernética do Brasil. Centro de Estudos Estratégicos do Exército: Análise Estratégica, v. 8, n. 2, p. 12-18, 2018.
MALHOTRA, Naresh K. Pesquisa de marketing: uma orientação aplicada. 4ª Ed. Porto Alegre: Bookman, 2004.
MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil. Artigo estratégico, v. 39, p. 1-14, 2018.
NEVES, José Luis. Pesquisa qualitativa: características, usos e possibilidades. Caderno de pesquisas em administração, São Paulo, v. 1, n. 3, p. 1-5, 1996.
PATHAK, Jagdish. Risk management, internal controls and organizational vulnerabilities. Managerial Auditing Journal, v. 20, n. 6, p. 569-577, 2005.
PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários a lei n 13.709/2018 (LGDP) – 2 ed. São Paulo: Saraiva Educação, 2020, 152p.
PSAVE Tecnologia S.A. Relátorio da Segurança Digital no Brasil – Terceito Trimestre – 2018. 2018. Disponivel em: https://www.psafe.com/dfndr-lab/pt-br/relatorio-da-seguranca-digital/. Acesso em: 19 Ago 2020.
Pfaffenzeller, Bruna. No rastro da corrupção praticada por pessoas jurídicas: da lei 12.846/2013 ao Projeto de Novo Código Penal. In: VITORELLI, Edilson (Org.). Temas atuais do Ministério Público Federal. Salvador. Juspodivm. 2015.
SANTOS, Viviane Bezerra de Menezes. Lei Geral de Proteção de Dados: Fundamentos e Compliance. 2019.
SHOPOS. THE STATE OF RANSOMWARE 2020: results of an independent study of 5,000 it managers across 26 countries. Results of an independent study of 5,000 IT managers across 26 countries. 2020. Disponível em: https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf. Acesso em: 31 jul. 2020.
STAFFORD, Thomas; DEITZ, George; LI, Yaojie. The role of internal audit and user training in information security policy compliance. Managerial Auditing Journal, n. 4, p. 410-424, 2018.
SECURITY, Cis Center For Internet. 10 principais malwares julho de 2020. 2020. Disponível em: https://www.cisecurity.org/blog/top-10-malware-july-2020/. Acesso em: 24 ago. 2020.
TREND MICRO. Smart Protection Network. Disponivel em: https://www.trendmicro.com/pt_br/business/technologies/smart-protection-network.html. Acesso em: 14 ago 2020.
WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos (2a. edição): Ameaças e procedimentos de investigação. Brasport, 2013.