XXIV SEMEAD
Seminários em Administração
novembro de 2021
ISSN 2177-3866

GESTÃO DE SEGURANÇA DE DADOS PESSOAIS: análise do impacto da lei geral de proteção de dados para as empresas

ANA CRISTINA ROCHA AGUIAR
UNIVERSIDADE SANTA ÚRSULA (USU)

MARINA FERNANDES DE OLIVEIRA
UNIVERSIDADE SANTA ÚRSULA (USU)

YANA TORRES DE MAGALHÃES
UNIVERSIDADE SANTA ÚRSULA (USU)

GESTÃO DE SEGURANÇA DE DADOS PESSOAIS:
análise do impacto da lei geral de proteção de dados para as empresas

1 INTRODUÇÃO

É inegável o quanto o uso da internet facilitou a relação de empresas com seus clientes, porém ao mesmo tempo atraiu criminosos em busca de informações pessoais e corporativas (GHAFIR, 2018). No último Fórum Econômico Mundial de Davos realizado em 2020, que reuniu líderes do G20, os cibercrimes foram citados como um dos grandes riscos para a economia do mundo (ABRANET, 2020). Na América Latina, o Brasil é o líder em número de cibe ataques, sendo o sétimo no ranking mundial de países mais atacados (RODRIGUES, 2019). Os próprios usuários estão se dando conta dos riscos: pesquisa realizada pelo Global Web Index relatou que 64% dos usuários da internet estão preocupados com a privacidade na rede e como empresas tratam seus dados (KEMP, 2020).

Em razão da preocupação mundial sobre a vulnerabilidade da internet e os riscos de vazamento de informações, diversos países começaram a pensar em como criar leis para a proteção do usuário (PIURCOSKY et al., 2019). A União Europeia criou, em 2016, o Regulamento Geral de Proteção de Dados - RGPD, implementado em maio de 2018 (UE, 2016). O RGPD visa à proteção da privacidade dos dados pessoais, prevendo responsabilização das empresas e inspirou diversos países na criação de novas leis. Dentre as alterações determinadas no regulamento, destacam-se a readaptação de softwares e o treinamento de equipes para que realizem operações de acordo com os princípios do regulamento (CORDEIRO; GOUVEIA, 2018).

No Brasil, a partir do Marco Civil da Internet, lei promulgada pelo Estado em 2014 (BRAGATTO, 2015), diversas leis e normas foram criadas para que empresas se responsabilizassem pela gestão de proteção de dados de clientes. A mais recente é a Lei Geral de Proteção de Dados - LGPD, Lei 13.709.2018, inspirada no RGPD. A LGPD determina os direitos dos titulares dos dados de acessarem judicialmente empresas que não realizarem um tratamento adequado de seus dados pessoais. A empresa passa a ser responsável por qualquer tipo de vazamento ou mau uso dos dados e, em caso de falta de adequação à LGPD, está sujeita a sanções administrativas, de advertências a multas de até cinquenta milhões de reais por dia (BRASIL, 2018).

Assim, se torna impreterível que empresas se adequem para cuidar da segurança dos dados que possuem, para evitar incidentes que comprometam até mesmo sua sustentabilidade financeira. Porém, um estudo recente realizado em Minas Gerais (PIURCOSKY et al., 2019) verificou que nenhuma das empresas mineiras pesquisadas estavam preparadas para atender às determinações da LGPD. Da mesma forma, pesquisa realizada entre junho e julho de 2020 com 400 empresas brasileiras verificou que 64% delas tampouco estavam adequadas à LGPD (ESTADÃO CONTEÚDO, 2020).

O presente estudo parte da verificação de que a LGPD, sendo recente, ainda é pouco conhecida, assim como seu impacto para as empresas. Em consulta ao site da Associação Nacional de Pós-Graduação e Pesquisa em Administração - ANPAD, em agosto de 2020, utilizando os termos “gestão de segurança de informação”, “segurança da informação”, “proteção de dados”, “administração de informação” e “Lei Geral de Proteção de dados”, foram encontrados apenas 21 artigos, sendo apenas um sobre a LGPD. Entre os 21 artigos encontrados na ANPAD, dois tratam exatamente da necessidade de aumentar estudos sobre gestão de segurança de informação.

Diante deste cenário, este estudo teve problema de pesquisa: qual o nível de adequação das empresas e de seus colaboradores à nova Lei Geral de Proteção de Dados (LGPD)? Definiu-se como objetivo geral analisar a adequação de empresas de segmentos diversos aos impactos

da Lei Geral de Proteção de Dados sob a perspectiva de seus colaboradores e de especialistas em gestão de segurança. A partir deles, foram definidos três objetivos específicos: verificar, sob a ótica dos especialistas, o impacto da LGPD nas empresas e as práticas para minimizar os riscos decorrentes; conhecer, sob a ótica dos colaboradores, as práticas adotadas pelas empresas para cumprimento dos princípios de segurança de informação e das determinações da LGPD; e analisar as práticas adotadas pelos próprios funcionários em relação à segurança da informação e à adequação à LGPD.

2 REVISÃO DE LITERATURA

2.1 Riscos por má gestão de segurança de dados e não adequação à Lei Geral de Proteção de Dados

Quanto mais vulneráveis as empresas, mais fácil é roubar, apagar ou editar dados na rede. Essa vulnerabilidade pode ser técnicas, processuais, humanas e em instalações (SILVA, 2010). Vulnerabilidade em gestão de segurança de dados pode ser entendida como falhas, riscos e fragilidades que as empresas vivenciam constantemente nos seus processos de negócios (LYRA, 2015).

As empresas estão investindo cada vez mais em tecnologias para diminuir essa vulnerabilidade, mas além do investimento em tecnologias é necessário mapear o tipo de informação que a empresa armazena e os riscos aos quais ela está sujeita, para cada tipo. De acordo com Torres e Foina (2015), essa análise deve fazer parte da estratégia de negócios da empresa, pois existem informações de domínio público, sem risco de vazamento, mas que requerem cuidados para que não sejam danificadas, e existem informações mais críticas que podem levar a empresa a perdas financeiras e até mesmo falência, como por exemplo informações de fusões, novos produtos e falhas graves. Ou seja, é preciso medir a importância de cada informação para a empresa. De acordo com Lyra (2015) quanto mais valiosa a informação, maior a probabilidade de ser alvo de ataques de cibercrimes. Com a Lei Geral de Proteção de Dados, as empresas passam a ser responsabilizadas também pelos dados pessoais de seus clientes, fornecedores e colaboradores, e os dados pessoais passaram a ser um forte alvo dos criminosos.

Para se ter segurança na proteção de dados de uma empresa, não basta investimento em tecnologias para proteção contra hackers e/ou antivírus, é necessário ainda preparar as pessoas. Pois assim como a vulnerabilidade, a gestão de segurança da informação pode ser dividida em três aspectos: tecnológico, físico e humano (SÊMOLA, 2003 apud NETTO ; SILVEIRA; 2007).

Em relação ao aspecto humano, o principal risco vem de ataques de engenharia social, técnica em que um intruso utiliza conhecimento do comportamento humano para conseguir informações da empresa (LYRA, 2015). A pessoa acaba sendo induzida ao erro e colocando a empresa em risco. Os hackers estão se especializando cada vez mais e utilizando métodos mais convincentes para induzir o operador de dados a baixar a segurança e permitir o acesso a dados. Segundo Torres e Foina (2015), um ataque de cibercrime pode fazer com que as operações da empresa fiquem totalmente paradas.

Cibercrime é todo ato que se utiliza de tecnologia de informação para realizar um ato criminoso (ALEXANDRE JÚNIOR, 2019). Alguns exemplos são ataques de *ransomware*, e outros *malwares* que visam interromper operações ou causar dano ao aparelho tecnológico, sistema ou rede, com potenciais diversificados como bloqueio de arquivos, fraudes eletrônicas, roubo de dados de cartão de crédito, venda de dados pessoais, envio de tipos de spam para e-mails corporativos (PEREIRA, 2017), que podem gerar penalidades por divulgação de dados pessoais, sobretudo com a criação da Lei Geral de Proteção de Dados.

A LGPD do Brasil e o RGPD da União Europeia determinam a responsabilização da

empresa em relação ao vazamento de dados dos clientes. No RGPD, as empresas ficam sujeitas ao pagamento de multa e devem comunicar o vazamento ao titular dos dados em até 72 horas (RIBAS; GUERRA, 2018). Na LGPD, o Art. 52 descreve as sanções administrativas às quais as empresas estão sujeitas em caso de descumprimento da norma:

> 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:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicitação da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019) (BRASIL, 2018).

As sanções da LGPD entrarão em vigor a partir de agosto de 2021 (BRASIL, 2018), porém caso ocorra algum vazamento de dado pessoal, desde agosto 2020, a vítima ou titular do dado pode entrar na esfera judicial contra a empresa. No site da Associação Nacional dos Profissionais de Privacidade de Dados já existem processos em andamento contra empresas que não seguiram os princípios da LGPD (ANPPD, 2020).

2.2 Práticas e ferramentas para adequação a LGPD e boa gestão de segurança de dados

Essa pesquisa não tem a intenção de exaurir todos os artigos da lei geral de proteção de dados, apenas destacar os pontos principais para análise dos objetivos propostos. Observa-se que a LGPD foi feita buscando a preservação da imagem e dos dados da pessoa física e tem como princípios respeito a privacidade, liberdade de expressão, autodeterminação, desenvolvimento econômico e tecnológico, livre iniciativa e direitos humanos (BRASIL, 2018). Também se baseou nos princípios de segurança de informação: confidencialidade, a qual garante que o acesso das informações é restrito a algumas pessoas e que há um controle; integridade, ou seja, a informação não deve ser adulterada e deve manter as mesmas condições entregues pelo titular dos dados; e disponibilidade, garantia que a informação do usuário está disponível para que ele visualize a qualquer momento (LYRA, 2015).

A LGPD regulamenta e orienta as empresas sobre o que é necessário fazer ou ter para que haja segurança no tratamento de dados pessoais. A lei define duas figuras que são responsáveis na empresa pelo tratamento de dados, denominados no Art. 6º, inciso IX, como agentes de tratamento: um é o controlador a quem competem as decisões em relação aos dados pessoais e o outro é o operador, quem realiza o tratamento dos dados (BRASIL, 2018).

Assim como no RGPD, a LGPD determina que somente com o consentimento do titular os dados podem ser tratados e apenas para a finalidade a que o titular autorizar (BRASIL, 2018). Por exemplo, os dados não podem ser transferidos de uma empresa para outra com uma finalidade diferente daquela para a qual o cliente deu o consentimento. O titular tem direito a ter acesso às informações que a empresa possui dele e solicitar a exclusão, devendo a empresa responder de forma clara todos os bancos de dados que possui e o prazo para exclusão. Caso não seja possível excluir, deve explicar o motivo (BRASIL, 2018).

De acordo com Torres e Foina (2015), para que haja uma correta segurança da informação é necessário um conjunto de boas práticas, como por exemplo elaboração de políticas de segurança, treinamentos e uso de ferramentas de controle. Além da LGPD, há outras normas brasileiras com relação direta ao tema segurança de dados. A Associação Brasileira de Normas editou em 2006 a NBR ISO/IEC 27001 e em 2013 a NBR ISO/IEC 27002, ambas Normas Técnicas para procedimentos de segurança de informação em empresas. Destacam-se aqui os pontos das normas que tem relação direta com o tema desta pesquisa. A NBR 27001 orienta a participação da diretoria no processo de segurança de informação, para assegurar que todos tenham competência e sejam informados sobre mudanças necessárias para minimizar os riscos de incidentes no tratamento de dados (ABNT, 2013a). Por sua vez, a NBR 27002 determina que a empresa tenha como procedimento a conscientização dos usuários sobre a segurança da informação (ABNT, 2013b). Ambas as normas sugerem também treinamentos e políticas organizacionais sobre segurança e proteção de dados.

Por esse motivo, é fundamental que as empresas desenvolvam ferramentas para criação de uma cultura de segurança de informação que leve em consideração seus funcionários. Afinal, o fator humano é um dos principais desafios para a implantação de boas práticas de segurança da informação em uma empresa (GHAFIR et al., 2018). Os treinamentos devem ser claros e repetidos periodicamente e a gerência deve controlar se os funcionários entenderam e estão seguindo as recomendações de segurança. Esses treinamentos não são apenas para repassar regras, mas sim para disseminar conhecimento (LYRA, 2015). Uma pesquisa de neurociência realizada em 2014 destacou que boa parte das pessoas esquecem em média 50% do conteúdo apresentado em um treinamento apenas uma hora depois de realizar o treinamento. Em 24 horas após o treinamento, uma pessoa pode esquecer 70% das informações e em uma semana, 90% do conteúdo (KOHN, 2014). Por esse motivo, e de acordo com Ghafir et al. (2018), é de extrema importância que "o treinamento de conscientização seja integrado às tarefas diárias dos funcionários, para apoiar a retenção e a aplicação do conhecimento adquirido". Ou seja, é fundamental contar com ações e treinamentos para formação e manutenção de uma cultura positiva e crescente, que eleve o nível da empresa (VARGAS, 2018).

Outro aspecto importante que a LGPD determina no artigo 55 é que devem ser realizadas auditorias para fiscalização de que o tratamento de dados nas empresas é realizado com diligência (BRASIL, 2018). A auditoria é uma das atividades principais de uma empresa para a garantia de que os processos estão sendo feitos da forma correta e evitar perdas, além de ser um instrumento de orientação para melhoria e redução dos riscos na gestão de segurança (RORATTO; DIAS, 2014).

Sem a cooperação dos operadores que irão realizar o tratamento de dados, é impossível garantir que os princípios de segurança serão cumpridos. Podemos usar como exemplo o fato de um funcionário deixar sua senha da rede anotada em local de fácil acesso e outro funcionário pegar indevidamente essa senha e acessar dados aos quais não tinha autorização. Sem o treinamento e a informação correta, o funcionário não toma os devidos cuidados para garantir a integridade, a confidencialidade e a disponibilidade que os princípios da segurança da informação demandam (LYRA, 2015).

A literatura evidencia que, com as mudanças impostas pela LGPD, se faz necessário que as empresas se adaptem a novos procedimentos de segurança e também conscientizem seus

funcionários da sua importância (PIURCOSKY et al., 2019). Porém, para que haja mudanças nas empresas é necessário que as pessoas mudem, pois elas são extremamente importantes nos processos organizacionais (FETZNER; FREITAS, 2012).

3 METODOLOGIA

Esta pesquisa de campo, de caráter empírico, é do tipo descritiva. De acordo com Triviños (1992), esse tipo de pesquisa busca verificar determinada situação, opiniões, fatos ou comportamentos, em uma determinada população. Neste estudo, a situação é a adequação de empresas de segmentos diversos aos impactos da Lei Geral de Proteção de Dados e para analisá-la opiniões de colaboradores e especialistas foram consideradas.

Quanto à abordagem, optou-se pela qualitativa. Conforme Vieira (2004), essa abordagem utiliza, com frequência, transcrições de entrevistas e de depoimentos que possibilitam oferecer diferentes pontos de vista, além de possibilitar obter descrições ricas, profundas e bem fundamentadas. Neste caso, usou-se a entrevista semiestruturada como ferramenta de coleta de dados, de forma a alcançar tal profundidade. As entrevistas foram gravadas e transcritas, com autorização dos participantes.

Para alcançar o primeiro objetivo específico, verificar sob a ótica dos especialistas o impacto da LGPD nas empresas e as práticas para minimizar os riscos decorrentes, foram entrevistados três especialistas da área de gestão de segurança, que estão envolvidos em projetos de adequação de políticas e práticas empresariais à LGPD. Para atender o segundo e o terceiro objetivos específicos foram entrevistados quinze colaboradores de três empresas que se adequam à LGPD, sendo cinco de cada empresa, para conhecer, sob sua ótica, as práticas adotadas pelas empresas para cumprimento dos princípios de segurança de informação e das determinações da LGPD, assim como identificar quais práticas são adotadas pelos próprios funcionários em relação à segurança da informação e à adequação à LGPD. As três empresas são privadas, de diferentes segmentos de atuação no Rio de Janeiro.

Tanto os especialistas quanto os colaboradores das três empresas foram definidos pelos critérios de tipicidade e conveniência. Segundo Vergara (2012), a amostra por tipicidade é constituída pela seleção de elementos que o pesquisador considere representativos da população-alvo. Os entrevistados estavam, no momento da coleta dos dados, envolvidos na adequação de adequação de políticas e práticas empresariais à LGPD. A conveniência, para Gil (2008), implica na escolha, pelo pesquisador, de recursos a que ele tem acesso, permitindo que estes possam, de alguma maneira, representar o universo. Nesta pesquisa, foram escolhidos especialistas, e colaboradores de empresas que, atendida a tipicidade, aceitaram participar do estudo.

Para analisar as entrevistas foi adotado o método de análise de conteúdo. Para Vergara (2012), análise de conteúdo é o tratamento do que está sendo dito ou lido sobre determinado tema, no caso dessa pesquisa, a adequação à LGPD. Foi tomado o cuidado de proteger a identidade dos entrevistados e das empresas, ainda mais sendo o tema deste estudo a segurança de informação e proteção de dados. Sendo assim, os especialistas serão chamados de Alfa, Ômega e Beta e as empresas de Verde, Azul e Amarela.

Quanto ao perfil dos especialistas entrevistados, o quadro 1, apresentado a seguir, apresenta a experiência de cada um em gestão de segurança, justificando a sua escolha para participar deste estudo, considerando o critério de tipicidade já mencionado.

Quadro 1: Identificação o perfil dos especialistas em gestão de segurança

Especialista	Descrição
Alfa	Perito em cibercrimes e atua em gestão de segurança de informação e proteção de dados. Presta consultoria a empresas do Rio de Janeiro há 6 anos, dedicado especificamente à melhoria de gestão de segurança de informação.
Ômega	Especialista em segurança de informação, trabalha nessa área há 10 anos e agora está responsável por conduzir o processo de adequação à LGPD de uma empresa de grande porte no segmento de transporte do Rio de Janeiro.
Beta	Analista de gestão de segurança e controle internos que atualmente está prestando consultoria para as empresas se adequarem à LGPD, com experiência de 11 anos em segurança de informação.

Fonte: Elaborado pelas autoras

Quanto ao perfil dos colaboradores das empresas, o quadro 2 apresenta a área de atuação, idade e número de funcionários das empresas e os cargos dos entrevistados.

Quadro 2: Informações gerais das empresas entrevistas e seus funcionários

Empresa	Descrição	Funcionário 1	Funcionário 2	Funcionário 3	Funcionário 4	Funcionário 5
Verde	Instituição de ensino superior. Possui 278 funcionários e 81 anos de atuação.	Atendimento	Coordenador de Central de Atendimento e Regulação Acadêmica	Coordenadora do Departamento Pessoal	Secretária Geral	Analista de TI
Azul	Empresa de importação e distribuição de insumos para indústria. Possui 71 funcionários e 83 anos de atuação.	Designer e Assistente de Marketing	Administra-tivo	Diretor Administra-tivo e Jurídico	Coordenador Técnico - Comercial	Supervisora de Vendas
Amarela	Consultoria empresarial para empresas e pessoas físicas. Possui 12 funcionários e 35 anos de atuação.	Gerente Comercial	Administra-tivo	Administra-tivo / Contas a pagar	Financeiro	Consultor Financeiro e Jurídico

Fonte: Fonte: Elaborado pelas autoras

As entrevistas foram realizadas de forma virtual através do aplicativo Zoom ou

Google Meet, por causa do distanciamento necessário para prevenção ao COVID-19, entre setembro e novembro de 2020 nos horários escolhido pelos entrevistados.

Foi utilizado roteiro semiestruturado, para assim haver uma liberdade maior para explorar com mais profundidade as respostas e com a autorização dos respondentes foi realizada a gravação do áudio das entrevistas. Ainda assim, a pesquisa apresenta limitações. Sendo uma amostra por acessibilidade, há o risco dos respondentes terem alterado suas respostas para atender a um suposto ideal. A amostra escolhida ainda tem outras limitações, pois não representa a totalidade de operadores de dados do Rio de Janeiro. Tampouco é uma amostra representativa que permita generalizações. Além disso, por tratar-se de um tema novo e ainda em implementação nas empresas, o acesso a quem trabalhe diretamente com gestão de segurança foi mais difícil, dada a sensibilidade das informações que podem ser passadas.

4 ANÁLISE DOS RESULTADOS

Nesse capítulo são apresentados os resultados das entrevistas realizadas com especialistas e funcionários da amostra de empresas do Rio de Janeiro. No subitem 4.1 estão os relatos dos especialistas e nos subitens 4.2 e 4.3 os relatos dos funcionários das três empresas estudadas.

4.1 O impacto da LGPD nas empresas e as práticas para minimizar os riscos decorrentes, sob a ótica de especialistas

Sobre o impacto que a LGPD irá trazer para as empresas em geral, os três especialistas concordaram que as empresas terão que realizar investimentos para se adequarem à nova lei. Todos ponderaram que dependendo do segmento da empresa e da quantidade de dados pessoais que utilizam, sejam de clientes, fornecedores ou funcionários, cada empresa será impactada de forma diferente, assim como a necessidade de investimento. Interpreta-se que o colhido nas entrevistas com os especialistas ratifica o referencial teórico, em que foi apresentado que será necessário fazer um mapeamento das informações pessoais que a empresa possui em todos os processos e investir tanto em tecnologia para melhor armazenamento dessas informações quanto em treinamento dos operadores que irão fazer o tratamento dos dados (ABNT, 2013a, 2013b; TORRES e FOINA, 2015; LYRA, 2015; PIURCOSKY et al., 2019).

No entanto, cada especialista complementou apontando um aspecto diferente do impacto. O Especialista Alfa destacou que as empresas deverão realizar um grande investimento financeiro para adequação à lei, principalmente porque no Brasil não se falava tanto em proteção de dados - apenas as grandes empresas ou instituições financeiras se preocupam há mais tempo sobre segurança de informação e estão mais preparadas. Para a Especialista Ômega, as relações comerciais serão as mais alteradas: as empresas deverão ter mais cuidado com os dados que recolhem de seus clientes e diminuir a base de dados conforme sua finalidade. Já o Especialista Beta enfatizou a necessidade de uma abordagem sistêmica, em que devem ser vistos todos os aspectos da gestão de risco, pois a gestão dos dados pessoais que uma empresa possui será tão importante quanto o gerenciamento de riscos financeiros. Pode-se relacionar todas essas falas ao defendido por Torres e Foina (2015), de que as empresas precisam pensar na adequação aos princípios de gestão de segurança como um pilar da estratégia de negócios, para assim evitar perdas e riscos.

Em relação aos riscos a que as empresas estão sujeitas caso não se adequem à LGPD, os três especialistas pontuaram multas e sanções administrativas, conforme descrito no Art. 52 da lei, apresentado no referencial teórico (BRASIL, 2018). Além disso, citaram outros riscos como processos judiciais de usuários contra a empresa, problemas de má reputação no mercado,

e a responsabilização da empresa mesmo que o vazamento seja por erro de terceiros, em caso de fornecedores. Segundo o Especialista Alfa, ainda que as sanções só entrem em vigor em agosto de 2021, já existem escritórios de advocacia se especializando em processos contra empresas baseados na LGPD, pois já podem haver punições na esfera judicial, dado que a lei já está em vigor. Além disso, possivelmente empresas com problemas de vazamento de dados terão seus nomes divulgados numa lista, na qual será categorizado o nível de adequação aos princípios da lei. A Especialista Ômega focou na prevenção, entendendo que as empresas precisam se antecipar para que, quando as sanções da LGPD estiverem em vigor, possam justificar estar de acordo com todos os princípios de adequação em caso de vazamento por culpa de terceiros. Finalmente, o Especialista Beta pontuou uma variedade de riscos em relação ao vazamento de dados, desde perda de credibilidade no mercado de ações e problemas de má reputação à classificação da empresa como não confiável.

Em relação às principais atividades que as empresas deverão fazer para que tenham as melhores práticas de adequação a LGPD, novamente os três concordaram que é importante que o trabalho de controle de dados pessoais seja inserido na rotina dos processos das empresas. Dentre as atividades de controle os especialistas citaram a auditoria, ratificando o que foi citado no referencial sobre esta ser uma das atividades principais para garantir que os processos estão sendo feitos da forma correta e evitar perdas, além de ser um instrumento de orientação para melhoria e redução dos riscos na gestão de segurança (RORATTO; DIAS, 2014). Lembra-se que no Art. 55 da LGPD é determinado que sejam realizadas auditorias n os processos de tratamento de dados (BRASIL, 2018).

Outra prática que os especialistas citaram para adequação foi o investimento em treinamento dos operadores. Segundo eles é fundamental, pois as pessoas são o elo mais fraco da gestão de segurança de informação. Para eles somente com um forte trabalho de conscientização e criação de uma cultura de proteção de dados em que todos os funcionários da empresa entendam sua importância será possível melhorar a gestão de segurança no aspecto humano. Essas falas corroboram novamente o referencial teórico, onde foi apresentada a vulnerabilidade humana na segurança de informação e a importância da conscientização de todos os funcionários (GHAFIR et al., 2018; SILVA, 2010; TORRES e FOINA, 2015; VARGAS, 2018).

O Especialista Alfa conta que realiza nas empresas um treinamento que além de explicar sobre os riscos e a boa gestão de segurança de informação também realiza práticas para testar o conhecimento, enviando simulações de ataques cibercrimes para que os funcionários vivenciem no seu dia a dia os conhecimentos aprendidos nos treinamentos. Esse procedimento concorda com o referencial teórico que propõe treinamentos claros e disseminadores de conhecimentos (LYRA, 2015).

Indo além, a Especialista Ômega pontuou que, para conscientização da LGPD nas empresas, é necessário o envolvimento da diretoria e de um grupo multidisciplinar, envolvendo diversas áreas da empresa com o mesmo objetivo de melhorar o tratamento de dados pessoais nos processos da companhia. Essa fala vem em acordo com a NBR 27001, que orienta a participação da diretoria no processo de segurança de informação, e com a NBR 27002, que determina que a empresa tenha como procedimento a conscientização dos usuários sobre as melhores práticas de gestão de segurança (ABNT, 2013a, 2013b).

4.2 Práticas adotadas pelas empresas para cumprimento dos princípios de segurança de informação e das determinações da LGPD, sob a ótica dos funcionários

Em relação ao conhecimento da Lei Geral de Proteção de Dados, dos 15 entrevistados das três empresas apenas um não sabia dizer do que se tratava e dois sabiam pouco e afirmaram ter pesquisado mais quando foram convidados para participar da entrevista. Porém, todos que disseram conhecer a LGPD afirmaram que conheceram a lei fora da empresa, em curso,

internet, jornais ou conversas com amigos. Segundo eles, a LGPD ainda não faz parte das suas rotinas nos processos de trabalho.

Esses relatos chamam a atenção, pois apesar da Lei Geral de Proteção de Dados estar em vigor desde setembro de 2020, as empresas, de acordo com os entrevistados, ainda não iniciaram o processo de conscientização dos funcionários. Mesmo aqueles que têm conhecimento sobre a lei, não o receberam dentro da empresa. Isso vem em desacordo com o encontrado no referencial teórico, o qual afirma a importância do treinamento, políticas de conscientização e comunicação clara e objetiva entre a empresa e seus funcionários (ABNT, 2013a, 2013b; PIURCOSKY et al., 2019; VARGAS, 2018).

Sobre os processos de adequação à LGPD realizados pelas empresas, todos os entrevistados indicaram uma percepção de que as empresas em que trabalham ainda não iniciaram nenhum trabalho para adequação à LGPD. Novamente, esta unanimidade chama a atenção, e remete ao cenário encontrado em estudos já citados, nos quais as empresas pesquisadas também não estavam preparadas para a LGPD (PIURCOSKY et al., 2019; ESTADÃO CONTEÚDO, 2020).

Alguns dos entrevistados não souberam informar o motivo das empresas não terem iniciado ações de adequação, porém entre aqueles que apresentaram justificativas destacam-se tanto a aplicabilidade da lei quanto a prorrogação do *vacatio legis*. No entanto, as justificativas não são fundadas. O Art. 3º da LGPD (BRASIL, 2018) declara que a lei se aplica a qualquer operação de dado pessoal em que o tratamento tenha por objetivo alguma atividade comercial como oferta de bens ou serviços. Sobre os pontos destacados pelos entrevistados das empresas Azul e Amarela, verifica-se que ambas correm o risco de sanções pela não adequação à lei, por falta de conhecimento no assunto. Pode-se supor, através desses relatos dos funcionários, que não estão tratando a segurança de informação como estratégico para o negócio, o que estaria em desacordo com o citado no referencial sobre a importância de manter boas práticas de segurança de informação (TORRES e FOINA, 2015).

Em relação ao treinamento sobre gestão de segurança de dados de dados pessoais, as três empresas apresentaram resultado parecido. Segundo o relato dos funcionários, nenhum recebeu treinamento sobre o assunto, porém os funcionários de cada empresa apresentaram justificativas diferentes. Os funcionários da Empresa Verde informaram que todo início de semestre tem conversas com os gestores, quando é reforçada a necessidade de se manter o cuidado com as informações de clientes e não transmitir para terceiros. Já os funcionários da empresa Azul acreditam que a Diretoria está preparando algo para apresentar para eles. Por último os funcionários da empresa Amarela afirmaram que, devido à pouca rotatividade, as informações são passadas diretamente entre gestor e funcionário, sem necessidade de um treinamento específico. Apenas quando um funcionário novo entra, é dito a importância de cuidar da privacidade de dados.

O treinamento é importante para que os funcionários sejam conscientizados da importância de manter boas práticas de segurança, conforme proposto nas normas NBR 27001 e NBR 27002. Também a Lei Geral de Proteção de Dados determina que a empresa tenha como procedimento a conscientização dos usuários sobre a segurança de informação (BRASIL, 2018). Indo além, Lyra (2015) propõe que os treinamentos devem ser realizados periodicamente, com uma comunicação clara para os funcionários e a gestão deve medir se os funcionários entenderam e estão seguindo as recomendações de segurança. Não foi encontrada nenhuma evidência dessas práticas, sob a perspectivas dos funcionários entrevistados.

Além do treinamento, foi apresentada a importância de divulgação de políticas sobre segurança de informação para todos os funcionários. Novamente, a unanimidade dos entrevistados das três empresas informaram que não possuem, ou não tem conhecimento da existência de políticas de segurança de informação. Porém, os funcionários das empresas Verde e Azul acreditam que provavelmente algo será divulgado em breve, pois já possuem outros

documentos que instruem boas práticas de comportamento, como códigos de éticas e instrução de atendimento. Em relação a empresa Amarela, os funcionários afirmaram que a empresa não divulga políticas ou documentos falando sobre conduta e desconhecem em especial sobre segurança de informação, pois acreditam que a empresa não necessita dessa formalidade uma vez que os funcionários são antigos e de confiança da diretoria. Tal fala contraria o que cita a NBR ISO/ IEC 27002 que cita treinamentos e criação de políticas como boas práticas de segurança que as empresas devem seguir (ABNT, 2013b).

Ainda buscando conhecer as práticas que as empresas pesquisadas estão utilizando para cumprimento dos princípios de segurança e adequação à Lei Geral Proteção de Dados, os entrevistados relataram se possuem processo de auditoria. A empresa Verde informou que periodicamente a Reitoria solicita dados para enviar à empresa mantenedora ou ainda é obrigatório o envio de registros acadêmicos para o MEC, mas uma auditoria específica para segurança de informação não há. Os funcionários da empresa Azul afirmaram que possuem processos de auditorias e que elas são fundamentais para que a empresa consiga ISOs[i] de Qualidade. Eles acreditam que assim que os processos da LGPD forem implementados haverá uma auditoria para comprovar se estão seguindo corretamente. Os funcionários da empresa Amarela afirmaram que ainda não passaram por nenhum processo de auditoria. Recapitulando o referencial, o processo de auditoria nas organizações é uma das atividades principais para a garantia de que os processos estão sendo feitos da forma correta e também serve como um instrumento de orientação para melhoria e redução dos riscos na gestão de segurança (RORATTO, DIAS, 2014).

Finalmente, na percepção dos funcionários as empresas já possuem algumas práticas de segurança de dados. Nas três empresas os sistemas exigem senhas e há um controle de acesso, seja por finalidade da área ou cargo. Na empresa Verde, por exemplo, os arquivos físicos de informações de funcionários somente podem ser acionados por dois funcionários do departamento pessoal. Um ponto positivo que se percebe analisando os relatos dos funcionários é que as empresas possuem controles tecnológicos de segurança, como o controle de acesso e senhas. Porém, é necessário pontuar que a elaboração de políticas de segurança, treinamentos e auditoria são peças fundamentais para que haja boas práticas de segurança (ABNT, 2006; TORRES e FOINA, 2015; LYRA, 2015; RORATTO; DIAS, 2014). Como já visto, sob a ótica dos seus funcionários, as empresas estudadas não contam com esses procedimentos.

4.3 Adoção de práticas pelos próprios funcionários em relação à segurança da informação e à adequação à LGPD

No referencial vimos que sem a cooperação dos operadores em manter boas práticas de segurança no tratamento de dados, é impossível atestar a segurança na informação (LYRA, 2015). Por esse motivo, é importante escutar os relatos dos funcionários sobre as práticas de segurança que utilizam.

Mesmo sem terem feito treinamentos específicos nas empresas sobre a LGPD ou sobre gestão de segurança, todos os entrevistados afirmaram que utilizam alguns princípios de segurança incentivados pelas empresas onde trabalham. Estes princípios foram transmitidos através de conversas individuais realizadas pelos gestores ou utilizando ferramentas tecnológicas disponibilizadas nos sistemas internos. Entre as práticas utilizadas pelos funcionários foram citados o uso de senhas complexas, controle de acesso por área, não divulgação de dados para terceiros e cuidado ao abrir e-mails com links desconhecidos. Dos 15 entrevistados apenas um não citou a utilização de senhas complexas. A não divulgação de dados pessoais para terceiros foi mencionado por 10 dentre os 15 entrevistados. Quanto ao controle de acesso por área, somente três pessoas apontaram isso como prática, e por último, o cuidado ao clicar em links de e-mails suspeitos foi citado por apenas dois entrevistados.

Pode-se interpretar que as empresas investiram em controle tecnológicos para minimizar

os riscos de vazamento de dados ou ataques de cibercrime, porém se o funcionário não os utilizar corretamente, não é possível garantir que serão eficazes. Como citado no referencial teórico, Lyra (2015) menciona a importância da cooperação dos operadores que irão realizar o tratamento de dados, pois a falta de treinamento e conscientização podem fazer com que uma falha humana gere um vazamento de dados.

Também é possível retirar dos relatos que 67% dos entrevistados citaram o cuidado em não transmitir informações para terceiros. Mesmo sem conhecerem profundamente os princípios da lei, essa prática está em acordo com o Art. 5 Inc. XII da LGPD, que determina que é necessário o consentimento do titular do dado para que seus dados sejam transferidos para terceiros (BRASIL, 2018). O Entrevistado 1 da empresa Verde contou sua experiência no atendimento em que um suposto pai solicitou os dados de uma aluna, o entrevistado verificou que não tinha informação desse responsável e negou transmitir a informação da aluna. Os entrevistados 2 e 3 também da empresa Verde contaram que é comum receber solicitações de ex-alunos por se tratar de uma instituição antiga, mas que eles têm como protocolo somente informar quando é assegurado por documentos que o solicitante é o titular do dado. Ainda na empresa Verde, a Entrevistada 4 afirmou que enquanto a Secretária Geral possui todos os dados dos estudantes, o setor de marketing possui apenas o e-mail institucional do aluno.

Da empresa Azul, os funcionários 3, 4 e 5 afirmaram que os acessos são controlados pelo cargo: a diretoria tem acesso a todas as informações, enquanto os cargos abaixo têm acesso apenas às informações compatíveis com suas responsabilidades. Essas atividades estão em consonância com o artigo 9º da LGPD que determina que deve haver uma finalidade específica para o tratamento de dados (BRASIL, 2018).

Apenas dois entrevistados, de diferentes empresas, contaram que estão atentos às solicitações através de e-mail, telefone ou presencialmente e zelam pela segurança dos dados confirmando quem é o solicitante para não passar dados indevidamente. A entrevistada 3 da empresa Amarela pontuou que sua gestora sempre alerta sobre a necessidade de conferir sites, e-mails e arquivos antes de abrir, para conferir sua veracidade. A entrevistada compartilhou que sempre utiliza essa prática, tanto na vida profissional quanto na vida pessoal. Essa é uma tentativa de minimizar os riscos de ataques de Engenharia Social (LYRA, 2015), que utilizam a vulnerabilidade do fator humano para acessar os dados nas empresas. O fato dos demais não terem citado essa prática de segurança pode ser tanto por não entenderem essa como uma prática de segurança quanto ser um indício de que necessitam mais cuidado em relação a possíveis ataques de Engenharia Social.

Finalizando, os entrevistados pontuaram a importância de compartilhar essa preocupação em segurança de informação para todos os integrantes das empresas, além de seus fornecedores e parceiros. Sobre esse ponto o Entrevistado 4 da empresa Verde defendeu que não basta o investimento em tecnologia, se não houver o esforço do funcionário em seguir os princípios de segurança de informação. O Entrevistado 5 da empresa Amarela reforça esta postura, dizendo que somente com um aculturamento de um pensamento em boas práticas de segurança será possível diminuir os riscos de vazamento de dados. Por último, a Entrevistada 1 da empresa Amarela disse que é necessário que haja transparência entre a diretoria e os funcionários para que qualquer problema de vazamento de dados seja logo comunicado para que os tratamentos possam ser realizados. Esses relatos estão em acordo com o que determina a NBR 27001 sobre a necessidade de toda diretoria nos processos de conscientização dos funcionários na boa gestão de segurança (ABNT, 2013a).

5 CONSIDERAÇÕES FINAIS

Com base nas entrevistas realizadas, atendeu-se ao objetivo da pesquisa, ao verificar-se que as empresas não estão adequadas à LGPD, apesar dos riscos aos quais estão submetidas.

No que diz respeito à de verificação do impacto da LGPD nas empresas e as práticas para minimizar os riscos decorrentes, os especialistas pontuaram que, além das sanções administrativas e multas previstas na lei, as empresas que não se adequarem correm risco de imagem e podem ter sua reputação abalada, uma vez que o cenário comercial mudará e a forma como as empresas lidarão com segurança de dados será avaliada pelo mercado. Além disso, ainda sob a ótica dos especialistas, as empresas devem investir não só em tecnologia para uma melhora gestão de dados, mas principalmente no treinamento dos operadores, pois o fator humano é o elo mais fraco na gestão de segurança e onde há maior vulnerabilidade. Outro aspecto destacado foi a necessidade de envolvimento da alta liderança organizacional para que haja mudanças efetivas.

Quanto às práticas adotadas pelas empresas para cumprimento dos princípios de segurança de informação e das determinações da LGPD, sob a ótica dos seus funcionários, destaca-se que nenhuma das três empresas havia realizado trabalhos para adequação da LGPD. Além disso, não realizaram treinamentos específicos sobre o tema. Como contraponto positivo, realizam controles tecnológicos de acesso de informações. Uma possível justificativa para o não treinamento pode ser a crença de que basta a proteção através de tecnologias, como as de acesso. Dessa forma, verificou-se que as empresas, até a conclusão desta pesquisa em novembro de 2020, não apresentaram as práticas propostas pela literatura, incluindo a própria LGPD, para sua conformidade com a lei. Em especial, ressalta-se a inexistência de treinamentos que permitam a criação de uma cultura de segurança de dados.

Por último, tratando da identificação das práticas adotadas pelos próprios funcionários em relação à segurança da informação e à adequação à LGPD, mesmo sem treinamento específico prévio, os funcionários das três empresas demonstraram saber a importância do cuidado com os dados de clientes, funcionários e fornecedores. Pode-se inferir que, por adotarem as medidas de segurança que são apresentadas pela empresa, como é o caso do uso de senhas de acesso complexas, os funcionários estariam propensos a seguir as orientações corporativas para atender princípios de segurança da informação.

Quadro 3: Resposta das empresas sobre práticas de segurança realizadas pelos funcionários.

Práticas de segurança realizadas pelos funcionários															
Empresa	**Verde**					**Azul**					**Amarela**				
Funcionário	**1**	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**
Senhas Complexas	-	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Controle de acesso por área	-	-	-	X	-	-	X	-	-	-	-	-	X	-	-
Não divulgação de dados para terceiros	X	X	-	-	X	-	-	X	X	-	X	X	X	X	X
Cuidado ao abrir e-mails	-	-	-	-	X	-	-	-	-	-	-	-	X	-	-

Fonte: Elaborado pelas autoras

Conclui-se que, em relação ao objetivo geral dessa pesquisa, de analisar a adequação de uma amostra de empresas aos impactos da Lei Geral de Proteção de Dados sob a perspectiva de seus funcionários e de especialistas em gestão de segurança, as empresas de forma geral serão impactadas pela LGPD e deverão realizar diversos investimentos para adequação. Sobre as empresas pesquisadas, de acordo com o relato dos funcionários, ainda necessitam fazer medidas nos processos de adequação à lei, em especial reforçar o treinamento, criar políticas sobre segurança e utilizar ferramentas de auditoria para controle dos processos.

Cabe ressalvar que, segundo os entrevistados, a pandemia da COVID-19 pode ter impactado nas medidas de conformidade à LGPD. Alguns processos das empresas foram alterados para priorizar o acesso remoto de funcionários, para que processos que antes eram

feitos apenas presencialmente, passassem a ser feitos digitalmente. Se por um lado a pandemia justifica o atraso na adequação à Lei Geral de Proteção de Dados, por outro lado ela intensifica sua necessidade, com um maior volume de dados circulando fora da proteção tecnológica da empresa pela prática de home office que se tornou necessária.

Para futuras pesquisas, sugere-se: aumentar a amostra de empresas entrevistadas; solicitar documentos das empresas estudadas para verificar as práticas de segurança não só na perspectiva dos funcionários, mas também por pesquisa documental; voltar às mesmas empresas entrevistadas nessa pesquisa após um ano e verificar se houve evolução em termos de adequação à LGPD e avaliar o impacto da pandemia do COVID-19 na adequação e nos riscos para a segurança e proteção de dados.

REFERÊNCIAS

ANPPD – ASSOCIAÇÃO NACIONAL DOS PROFISSIONAIS DE PRIVACIDADE DE DADOS. **Portal das violações-LGPD**. Disponível em: https://anppd.org/violacoes. Acesso em: 08 nov. 2020.

ABRANET – ASSOCIAÇÃO BRASILEIRA DE INTERNET. **Fórum Econômico Mundial adverte que desigualdade digital é um risco para humanidade**, 16 jan 2020. Disponível em: https://www.abranet.org.br/Noticias/Forum-Economico-Mundial-adverte-que-desigualdade-digital-e-um-risco-para-a-humanidade-2710.html?UserActiveTemplate=site#.YLk9gy35RpQ. Acesso em: 06 abr. 2020.

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

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:** Tecnologia da informação, Técnicas de segurança, Código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013b.

ALEXANDRE JÚNIOR, Júlio César. Cibercrime: um estudo acerca do conceito de crimes informáticos. **Revista Eletrônica da Faculdade de Direito de Franca**, v. 14, n. 1, p. 341-351, 2019.

BRAGATTO, Rachel Callai; SAMPAIO, Rafael Cardoso; NICOLÁS, Maria Alejandra. A segunda fase da consulta do marco civil da internet: como foi construída, quem participou e quais os impactos. **Revista Eptic**, v. 17, n. 1, p. 237-255, 2015.

BRASIL. **Medida provisória nº 959, de 29 de abril de 2020**. Dispõe sobre a operacionalização do pagamento do Benefício Emergencial de Preservação do Emprego e da Renda e do benefício emergencial mensal de que trata a Medida Provisória nº 936, de 1º de abril de 2020, e prorroga a vacatio legis da Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais – LGPD, 2020. Brasília, DF. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Mpv/mpv959.htm. Acesso em: 01 abr. 2020.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF, [2018]. Disponível em http//www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm#art65. Acesso em: 01 abr. 2020.

CORDEIRO, Silvério; GOUVEIA, Luis Borges. Regulamento Geral de Proteção de Dados (RGPD): o novo pesadelo das empresas? **Relatórios Internos* TRS**, v. 2018, n. 07/2018, 2018.

ESTADÃO CONTEÚDO. Pesquisa indica que 64% das empresas não estão em conformidade com a LGPD. **Infomoney**, 29 ago 2020. Disponível em: https://www.infomoney.com.br/economia/pesquisa-indica-que-64-das-empresas-nao-estao-em-conformidade-com-a-lgpd/. Acesso em: 14 nov. 2020.

FETZNER, Maria Amélia de Mesquita; FREITAS, Henrique Mello Rodrigues de. Repensando questões sobre mudança, afeto e resistência na implementação de SI. **REAd. Revista Eletrônica de Administração (Porto Alegre)**, v. 18, n. 1, p. 1-26, 2012.

GHAFIR, Ibrahim; SALEEM, Jibran; HAMMOUDEH, Mohammad; FAOUR, Hanan; PRENOSIL, Vaclav; JAFL, Sardar; JABBAR, Sohail; BAKER, Thar. Security threats to critical infrastructure: the human factor. **The Journal of Supercomputing**, v. 74, n. 10, p. 4986-5002, 2018.

GIL, Antônio C. Métodos e Técnicas de Pesquisa Social. São Paulo: Atlas, 2008.

KEMP, Simon. **Digital 2020:** Global Digital Overview. Disponível em: https://datareportal.com/reports/digital-2020-global-digital-overview. Acesso em: 09 jun. 2020.

KOHN, Art. **Brain science:** the forgetting curve–the dirty secret of corporate training. v. 7, 2014.

LYRA, Mauricio Rocha (org). **Governança da segurança da informação**. Brasília: nd, 2015.
NETTO, Abner da Silva; SILVEIRA, Marco Antonio Pinheiro da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. **Journal of Information Systems and Technology Management**, vol. 4, no. 3, São Paulo, 2007. https://doi.org/10.1590/S1807-17752007000300007.

PIURCOSKY, Fabrício Peloso; COSTA, Marcelo Aparecido Costa; FROGERI, Rodrigo Franklin; CALEGARI, Cristina Lelis Leal. A Lei Geral de Proteção de Dados Pessoais em empresas brasileiras: uma análise de múltiplos casos. **Suma de Negócios**, v. 10, n. 23, p. 89-99, Julio-Diciembre 2019. ISSN 2215-910X. Doi: http://dx.doi.org/10.14349/sumneg/2019.V10.N23.A2

RIBAS, Brenno Henrique de Oliveira; GUERRA, Carolinne Cardoso. **O impacto do regulamento geral de proteção de dados pessoais da União Europeia no Brasil.** Governança e direitos fundamentais, p. 75. 2018.

RODRIGUES, Renato. Internauta brasileiro sofre 22 ataques por segundo. **Kapersky Daily**, 28 ago 2019. Blog. Disponível em: https://www.kaspersky.com.br/blog/brasileiro-22-ataques-segundo-klsec/12239/ . Acesso em: 23 mai. 2021.

RORATTO, Rodrigo; DIAS, Evandro Dotto. Security information in production and operations: a study on audit trails in database systems. **JISTEM - Journal of Information Systems and Technology Management**, v. 11, n. 3, p. 717-734, 2014.

UE – UIÃO EUROPEIA. Serviço das Publicações da União Europeia. Regulamento Geral sobre a Proteção de Dados. **Jornal Oficial da União Europeia**, L119, 59º ano, 4 de maio de 2016. ISSN 1977-0774 (edição eletrônica). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=PT . Acesso em: 25 abr. 2020.

SILVA, Abner de Oliveira e. Engenharia social: o fator humano na segurança da informação. **Coleção Meira Mattos: revista das ciências militares**, n. 23., CMM/PADECEME 3º Quadrimestre de 2010. ISSN 2316-4891.

TORRES, Fabio Cabral; FOINA, Paulo Rogerio. Conceitos e princípios da segurança da informação. *In*: LYRA, Mauricio Rocha. (org.). **Governança da Segurança da Informação**. Brasília: nd, 2015. p. 259-261.

TRIVIÑOS, A.N.S. **Introdução à Pesquisa em Ciências Sociais.** São Paulo: Atlas, 1992.

VARGAS, Rodrigo. **Cultura de Melhoria**: Levando a Organização á Excelência. São Paulo: Portuguese Edition, 2018.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa.** São Paulo: Atlas, 2012.

VIEIRA, M.M.F. Por uma boa pesquisa (qualitativa) em Administração. In: VIEIRA, M.M.F.; ZOUAIN, D.M. Pesquisa qualitativa em Administração. Rio de Janeiro: FGV, 2004.

[i] ISO é a sigla de International Organization for Standardization, uma organização criada na Suíça com o propósito de padronizar normas para serem utilizadas em todo o mundo. Neste contexto refere-se às certificações empresariais segundo a ISO.