LGPD: DIAGNÓSTICO DE EMPRESAS PARA ADEQUAÇÃO ÀS NORMAS DA LEI Nº 13.709

Christian Warmling Medeiros[1]

Rogerio Herminio Da Silva[2]

Resumo: A Lei Geral de Proteção de Dados foi promulgada em 2018 com intuito de atender as exigências do mercado global e proteger os dados de pessoas físicas, tendo em vista que empresas têm aproveitado para lucrar com dados alheios sem que o titular perceba. Ainda que tenha sido escrita anos atrás, entrado em vigor em 2020 e com suas sanções administrativas passando a valer para o segundo semestre de 2021, muitas empresas sequer têm conhecimento sobre ou não sabem se estão dentro dos padrões para conformidade. Dentro desse contexto, o trabalho tem como finalidade realizar um diagnóstico em uma empresa para calcular o grau de conformidade e então analisar cada índice e elaborar uma recomendação para que a empresa possa começar o processo de conformidade. Para atingir o objetivo foi disponibilizado um questionário com 10 perguntas para 30 empresas. Destas 30 empresas 17 responderam ao questionário e uma foi selecionada para realização do diagnóstico. A pesquisa foi realizada em duas etapas por meio de um questionário composto por 113 perguntas. A pesquisa é útil para identificar o nível conformidade geral das empresas e validar o diagnóstico através da sua aplicação em uma empresa.

Palavras-chave: LGPD. Privacidade. GDPR. Diagnóstico.

1 INTRODUÇÃO

Pode parecer um assunto atual, o que de fato é, mas questões sobre privacidade datam muito antes de os telefones popularizarem e surgir a primeira escuta telefônica. Em 1890 o advogado Louis Brandeis já previa que informações pessoais pudessem ser reveladas para satisfazer outros fins e como a evolução das máquinas ameaçam o direito do indivíduo de “ser deixado em paz” (BURROWS, 2013). A primeira referência que se tornou como base para que o mundo considerasse a privacidade um direito fundamental para o ser humano veio da Declaração Universal

[1] Graduando em Eng. da Computação do Centro Universitário UNISATC. 2021/1 E-mail: christianwmedeiros@outlook.com

[2] Prof. do Centro Universitário UNISATC. E-mail: rogerio@protectsolutions.com.br

dos Direitos Humanos, na qual no artigo 12º destaca que “ninguém será sujeito a interferência arbitrária em sua privacidade, família, casa ou correspondência, nem a ataques à sua honra e reputação” (ONU, 1948). Assim como também no artigo 5º da Constituição Federal cita que a vida privada e a intimidade da pessoa devem ser preservadas, que em caso de violação assegura-se o direito à indenização (BRASIL, 1988).

O primeiro conceito que leva o nome de “Lei de Proteção de Dados” entrou em vigor em 1971 em um estado da Alemanha, logo após isso países como Estados Unidos e Suécia aprovaram suas próprias leis (HOLVAST, 2009). Anos mais tarde surgiram outros textos regulamentando suas leis em seus respectivos países, entre os mais famosos destaca-se a *California Consumer Privacy Act* (CCPA) da Califórnia e a *General Data Protection Regulation* (GDPR), regulamentação da União Europeia (POHLMANN, 2019).

Esta foi escrita em 2016 e entrou em rigor em 2018, os primeiros textos já destacam não somente o respeito proveniente ao tratamento de dados como “respeitar os seus direitos e liberdades fundamentais, em particular o seu direito à proteção dos dados pessoais” (EU, 2016). A GDPR serviu de inspiração para o mundo, em especial para o Brasil, formalizando assim a Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2020).

A LGPD (Lei nº 13.709, de 14 de agosto de 2018) foi promulgada para a proteção de dados pessoais e regulamentar o “tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado” seja em operações nos meios manuais ou digitais cuja finalidade seja para fins comerciais (BRASIL, 2020). No texto oficial e nos guias disponibilizados pelo governo federal, como o Guia de Elaboração de Programa de Governança em Privacidade, é possível identificar os personagens envolvidos em cada etapa, os direitos do titular, as consequências em caso de não cumprimento da lei e algumas outras orientações (BRASIL, 2020).

Assim como afirma Margrethe Vestager, em entrevista para o site Recode, há muitas empresas que lucram com a venda ou uso de dados pessoais para o marketing e outros afins, destacando que não há serviços totalmente gratuitos (JOHNSON, 2016). Por isso a importância da conformidade com a LGPD nas empresas, seja para proteção do titular dos dados pessoais seja para a instituição que

faça qualquer tipo de tratamento de dados estejam reguladas para receber essas informações (RIVELLI, 2020).

Para estar em conformidade com a lei é preciso realizar algumas medidas como nomeação dos indivíduos responsáveis por cada área, como o controlador operador e encarregado, alinhamento e treinamento básico da alta gestão e colaboradores, análise da maturidade e análise e adoção de medidas de segurança (BRASIL, 2020).

O presente trabalho estrutura-se em realizar pesquisa com micro até médias empresas do sul do estado de Santa Catarina para identificar os problemas recorrentes que podem afetar a busca pela conformidade com a LGPD, assim como ajudará a encontrar uma empresa que se enquadra em desconformidade para que a etapa de diagnóstico seja realizada.

Propondo-se então, realizar um diagnóstico com a empresa escolhida para calcular um índice que às ajudará a reconhecer os pontos fracos da sua conformidade com a Lei Geral de Proteção de Dados e entregá-los recomendações para cada caso.

Ao final deste artigo levanta-se os resultados obtidos, o caso analisado e as recomendações enviadas para a empresa.

2 REFERENCIAL TEÓRICO

Como já mencionado, a LGPD não foi iniciada do zero assim como para relações internacionais não é a única regulamentação que deve ser seguida. Depois de colocado em vigor o regulamento da União Europeia, as dificuldades de continuar fazendo negócios com a Europa aumentaram, sendo assim no Brasil houve pressa em promulgar uma legislação adequada sobre proteção de dados (POHLMANN, 2019).

De certo modo, assim que qualquer negócio envolver clientes fora do Brasil é necessário estar de acordo com a legislação em que o cliente está, logo se um site brasileiro aceitar negócios que vierem da Europa será necessário seguir a GDPR (POHLMANN, 2019). Por esse motivo, também pela GDPR ter sido promulgada antes de qualquer legislação, a LGPD tomou-a como inspiração base e esse é o motivo da importância de conhecer mais a fundo as normas da União Europeia.

2.1 GDPR

É correto afirmar que desde dezembro de 2015, quando o Parlamento Europeu e Conselho firmaram o acordo, as relações e estratégias de mercado foram impactadas e isso ocorreu internacionalmente, envolvendo até mesmo gigantes como Google e Facebook (ALBRECHT, 2016). Em seus primeiros capítulos e artigos destaca-se o foco em proteção de dados pessoais de pessoas físicas, exigindo que os dados coletados devem ser adequados somente ao que é estritamente necessário e processado de forma lícita e transparente (EU, 2016).

No que se diz a respeito do tratamento ou processamento, somente será permitido com o consentimento do titular dos dados e apenas para tarefas que se designem ante o acordo com o titular. Caso o tratamento tenha outra finalidade do que foram propostos inicialmente para o titular, o responsável pelo tratamento deve analisar se o objetivo não extrapola o contexto do acordado e deverá estar sujeito a possíveis consequências (EU, 2016).

O consentimento com o titular deve ser claro e objetivo, salvaguardando que em qualquer momento ele pode retirar o acordado sem afetar a legalidade do processamento antes da retirada, o titular deve ser informado desse direito e a retirada ser tão fácil quanto a entrada de dados (EU, 2016).

Outras regras que podem ser resumidas são a respeito de dados de titulares menores idade, onde nesse caso a autorização deve partir de um responsável maior, e tratamento de dados relativos a condenações criminais ficam responsabilizados pelo Estado, sempre respeitando os direitos e liberdades dos titulares (EU, 2016).

Outras normas parecidas também se encontram na LGPD, mudando algumas poucas coisas. Segundo a norma, em caso de infração as multas variam, de modo geral a empresa que cometer irregularidades deverá pagar 20 milhões de euros ou 4% do faturamento anual (EU, 2016).

A fiscalização e aplicação de multas começou em 25 de maio de 2018, dia em que entrou em rigor (POHLMANN, 2019).

2.2 LGPD

Desde que a GDPR entrou em rigor, surgiu necessidade de o Brasil acompanhar as exigências da União Europeia bem como os regulamentos de outros países, fator importante para não perder negócios e clientes. Até por isso, a Lei Geral de Proteção de Dados pode se parecer um pouco com a regulamentação europeia (POHLMANN, 2019).

Apesar disso, a lei nº 13.709 mostrou-se robusta e com algumas exigências e responsabilidade a mais (POHLMANN, 2019).

2.2.1 Lei

O texto começa destacando sobre sua finalidade, nada muito diferente do que se apresentou nesse presente artigo até então, vale mencionar que a lei se aplica em tratamento de dados realizado por pessoa natural ou jurídica desde que a operação seja realizada em território nacional. Sendo que não se aplica quando o tratamento ocorre para fins particulares ou não econômicos, jornalísticos, acadêmicos e atividades que envolvam o trabalho do Estado (BRASIL, 2018).

Resumindo-se alguns pontos de destaque, se encontra sobre dado pessoal, em vista da Lei, é informação relacionada a pessoa física identificada ou identificável, o que não se enquadra a isso são informações sobre a saúde, origem racial, convicção religiosa, opinião política e outros dados que remetem a dados pessoais sensível (BRASIL, 2018).

Podem ocorrer casos de dado anonimizado, permitindo a utilização de meios técnicos razoáveis quando o titular não possa ser identificado, algo parecido com a anonimização, processo no qual se perde a associação direta ou indireta do indivíduo (BRASIL, 2018).

Assim como consta Brasil (2018, Art. 5) destaca-se que o tratamento se refere a:

> Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

E essa ação só pode ocorrer mediante o consentimento do titular, em situações de cumprimento de obrigações legais, realizações de estudos e proteção da vida do titular são casos em que o tratamento de dados se enquadra. De toda maneira o titular tem o direito de saber com facilidade a finalidade para qual seus dados estão sendo coletados (BRASIL, 2018).

Até esse ponto, é importante salientar que aos olhos da LGPD “todo e qualquer dado pessoal deve ser protegido, independentemente do meio pelo qual o mesmo seja obtido ou processado” (POHLMANN, 2019). Dessa forma o controlador deve realizar o tratamento apenas para a promoção da atividade legitima do controlador e proteção do titular (BRASIL, 2018).

O tratamento considera-se terminado quando a finalidade para o qual os dados foram coletados foi alcançada, o prazo e acordo finalizado ou a pedido do titular para transferência ou exclusão (BRASIL, 2018).

O titular também tem o direito de saber qual a utilidade de seus dados, isso deve ser informado antes da coleta. Assim como deve ser fácil ter acesso aos seus dados, pedir informações sobre o controlador e a eliminação, bloqueio ou transferência dos dados (BRASIL, 2018).

No que tange ao poder público, somente é permitido o tratamento desde que não infrinja a privacidade do titular, sob atividade legais que remetem a lei. Já a transferência internacional de dados só poderá acontecer caso o país ao qual os dados serão destinados tenha também uma regulamentação aceitável (BRASIL, 2018).

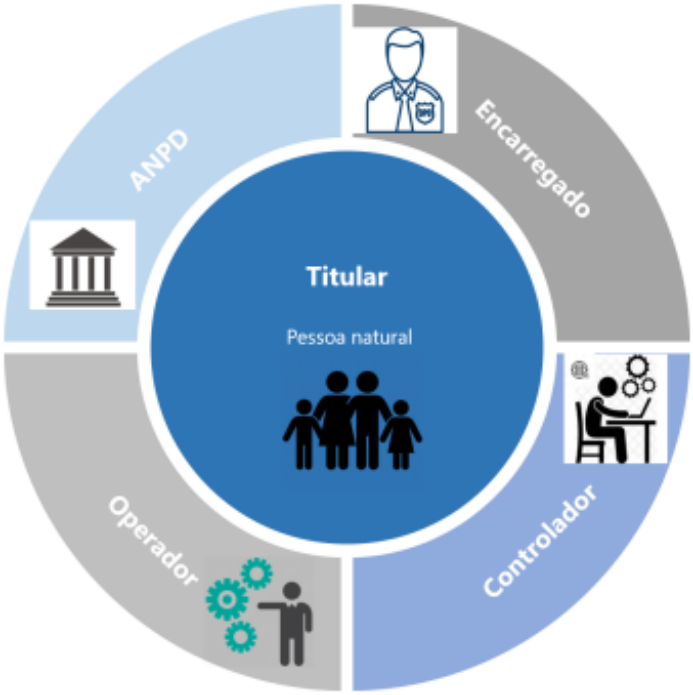
2.2.2 Agentes de dados

No regulamento da LGPD há informações acerca dos agentes que englobam a coleta e tratamento de dados. Já se tem mencionado neste presente artigo sobre o titular, que representa a pessoa natural, assim como o controlador.

O controlador é a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (BRASIL, 2018). Pode-se dizer que é basicamente o dono do banco de dados dentro de limites legais.

Para realizar o tratamento precisa-se do operador, semelhante ao controlador, com a diferença de que esse realiza as ações em nome do controlador (BRASIL, 2018). Nesse sentido, é aquele que realiza a ação e muitas vezes o controlador e o operador podem ser a mesma pessoa (POHLMANN, 2019). A figura 1 relaciona os agentes citados.

Figura 1: Atores LGPD



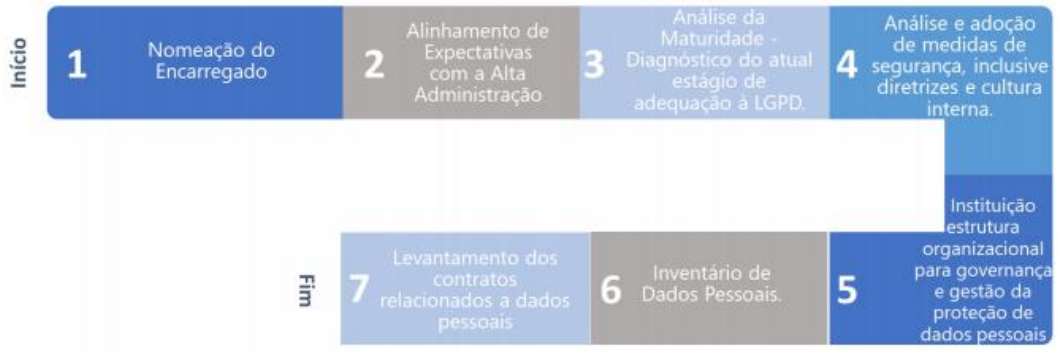
Fonte: Brasil (2020)

Há um terceiro agente, esse responsável pela comunicação com o titular, controlador e a Autoridade Nacional de Proteção de dados, que se denomina encarregado. Pohlmann (2019) entende que o encarregado não é exatamente um cargo de alta complexidade e escalão, mas alguém escolhido pelo controlador e operador para suas funções, em alguns casos podendo até ser um deles.

2.2.3 Planejamento e execução de conformidade à Lei

Em 2020 o governo federal disponibilizou alguns documentos para servir de guia para estar de acordo com o regulamento, na figura 2 encontra-se o caminho sugerido para a adequação.

Figura 2: Planejamento



Fonte: Brasil (2020)

Por meio do fluxo sugerido pelo governo federal deve-se primeiramente fazer a nomeação do agente encarregado, sendo aquele que realizará todo o processo junto às bases legais. Em segundo momento indica-se fazer um alinhamento com a alta gestão e determinar as prioridades de suas ações (BRASIL, 2020).

Para avançar é preciso analisar o quanto a empresa está madura no que condiz a conformidade da LGPD, como a elaboração da política de privacidade e termos de uso de serviços. Na etapa seguinte revisa-se a cultura interna e aplica-se as boas práticas da LGPD (BRASIL, 2020).

Os três últimos passos consistem em estabelecer a estrutura recomendada, obter o mapeamento de dados, este irá documentar o tratamento de dados pessoais realizados pela instituição, e por fim, o último passo “contribui para possíveis e necessárias adequações contratuais, tanto nos contratos existentes, quanto nos futuros” (BRASIL, 2020).

2.2.4 Monitoramento de atividade e conformidade da empresa

O acompanhamento contínuo da conformidade à LGPD é de extrema importância, assim essa etapa também aborda alguns passos importantes, como pode-se observar no fluxo sugerido pelo governo federal presente na figura 3.

Figura 3: Monitoramento

Fonte: Brasil (2020)

No fluxo acima observa-se 4 importantes etapas que marcam o início e fim de cada ciclo de monitoramento, é importante lembrar que essa prática é continua e não se realiza apenas uma vez, o está de acordo no que afirma Pohlmann (2019) que defende a importância de criar métodos automatizados que monitorem de forma constante.

O primeiro passo que consta no fluxograma presente na figura 3 aborda a performance da política adotada pela empresa, nessa parte avalia-se alguns critérios como o acompanhamento no número de incidentes de violação e/ou vazamento de dados pessoais, resultados de diagnóstico de adequação à lei e cálculo de índices de serviços referente aos processos realizados (BRASIL, 2020).

A segunda etapa consiste em relatar os incidentes ocorridos fazendo uma descrição dos eventos, dos sistemas envolvidos, as medidas de segurança utilizadas, os riscos relacionados ao incidente assim como as medidas tomadas a fim de evitá-los (BRASIL, 2020).

Por fim resta analisar os resultados e fazer o reporte deles nas duas últimas etapas, como o objetivo de “mostrar a evolução das ações e resultados obtidos, bem como o papel da privacidade para o cidadão reforçam e fortalecem a cultura de privacidade dos dados” (BRASIL, 2020).

Para auxilio da empresa nessa etapa é interessante obter a certificação ISO/IEC 27701, este padrão internacional é uma extensão da ISO/IEC 27001 e 27002 e com ela promete simplificar essa etapa de monitoramento de forma que a instituição por meio da norma faça a reconciliação de vários requisitos regulamentares, economize ao auditar cada regulamentação e melhorar acordos comerciais com a garantia da certificação para tornarem-se mais confiáveis com relação ao tratamento de informações pessoais (ABNT, 2019).

2.2.5 Infrações e desconformidades perante a Lei

A Lei Nº 13.709 entrou em vigor em 18 de setembro de 2020 enquanto suas sanções administrativas passarão a valer a partir de 1 de agosto de 2021, sendo assim os agentes de tratamento de dados que não estiverem em conformidade estarão sujeitos à uma série de limitações e punições (BRASIL, 2018).

Logo no primeiro artigo da seção de sanções administrativas destaca-se que em caso de infrações as instituições serão notificadas com advertência, recebendo um prazo para adotar as medidas corretivas. Além de ser cobrada multas diárias em 2% do faturamento, com limite de R$ 50 milhões para cada infração (BRASIL, 2018).

A maioria das punições se referem às atividades que tenham relação aos dados pessoais, como o bloqueio destes até a regularização da empresa ou mesmo a eliminação dos dados pessoais que tenham relação com a infração. Há outras atividades que podem ser comprometidas pois além dessas citadas tem mais punições que levam a suspensão parcial do funcionamento do banco de dados, suspensão do exercício da atividade de tratamento dos dados pessoais e proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (BRASIL, 2018).

Ainda assim, o infrator tem a oportunidade de defesa que deverá ser considerado alguns critérios como a gravidade e a natureza das infrações e seus graus de danos, a boa-fé bem como a vantagem pretendida pelo infrator, a adoção de política de boas práticas, a adoção de medidas corretivas e procedimentos internos capazes de minimizar o dano (BRASIL, 2018).

3 METODOLOGIA

Em primeiro momento obteve-se conhecimento sobre a LGPD no decorrer do curso destacando sua importância no cenário atual, também se contou com o apoio de artigos e demais documentos para aprofundamento vide as referências desse respectivo trabalho. Decidiu-se realizar duas abordagens, primeiramente realizar uma pesquisa de status de conformidade para levantar dados e obter-se noção da

deficiência das empresas com relação à conformidade com a LGPD, seja no tratamento de dados ou na adoção de medidas de segurança, em razão de a LGPD atingir todo nicho de empresa sem importar seu tamanho a pesquisa foi destinada à empresas de micro até médio porte para facilitar a coleta de dados, a pesquisa serviu também para identificar e escolher uma empresa para proceder com a etapa de diagnóstico. Etapa essa que envolveu a realização de uma parte prática do conhecimento teórico junto à empresa escolhida, a atividade prática trata-se de uma realização de um diagnóstico que ajudou a empresa no processo inicial para a conformidade à Lei.

3.1 PESQUISA GERAL DE CONFORMIDADE E VALIDAÇÃO DO PROBLEMA

Com a ajuda de um questionário, realizou-se a pesquisa de forma a identificar os principais problemas das empresas que comprometam a conformidade com a LGPD.

Em primeiro momento salienta-se que será divulgado o resultado geral e não o que cada empresa respondeu, garantindo que nenhuma será prejudicada pelas respostas dadas. O questionário começou com um breve resumo sobre o que é a LGPD e o que mudou com a Lei, além de tratar da questão prática do trabalho.

As perguntas foram realizadas de maneira a identificar dificuldades ou problemas relacionados à área de privacidade de dados pessoais e como a empresa se comporta nesse quesito, todas foram elaboradas com base no trabalho de Silva (2021). Ressalta-se que foi destacado que nenhuma das 10 perguntas, podendo ser respondidas com sim ou não, possuem respostas certas ou erradas e recomendou-se para que fossem respondidas conforme a realidade das empresas.

As perguntas foram realizadas da seguinte forma:

1) Na sua empresa há um controle contra riscos de segurança da informação?
2) Na sua empresa há um controle de acesso aos arquivos tanto físico quanto digital?
3) Na sua empresa possui uma política de segurança da informação que esteja de acordo com as necessidades do negócio?
4) Os colaboradores da empresa têm treinamento de conscientização sobre segurança da informação?

5) Na sua empresa possui política de backup para restauração dos dados armazenados caso haja algum desastre?
6) Os colaboradores que trabalham remotamente são gerenciados com segurança pela empresa?
7) Sua empresa possui firewall para proteção dos dispositivos contra ataques e ajudar a evitar a violação de dados?
8) Possui anti-malware com gestão centralizada para proteger os dispositivos contra malwares?
9) Os tomadores de decisão da empresa promovem uma cultura positiva de conformidade de proteção de dados em toda a empresa?
10) A empresa usa os dados obtidos para outras finalidades além do que foi proposto inicialmente?

Para a coleta de dados enviou-se o questionário por e-mail às empresas, reforçando o contato por telefone para obter as respostas e ao final do questionário disponibilizou-se um espaço para que pudessem informar contato direto com a finalidade de realizar a etapa de diagnóstico.

3.2 DIAGNÓSTICO DE CONFORMIDADE EM UMA EMPRESA

O procedimento começou com o primeiro contato com as empresas que deixaram o e-mail para proceder com a etapa de diagnóstico e escolheu-se uma delas seguindo os critérios de estar em desconformidade com a lei, analisado através da pesquisa em que se identificou problemas quanto a segurança de dados pessoais, e disponibilidade de tempo para a realização do questionário.

Usufruindo de o autor já ter contato direto com os sócios da empresa escolhida, realizou-se uma reunião com a alta gestão para conhecer a atividade da empresa, repassar o conhecimento e relatar as métricas da LGPD. Salienta-se que para relatar ao máximo a procedência da pesquisa foi autorizado a divulgação dos dados bem como o nome da empresa nessa etapa.

Vale lembrar que o procedimento de diagnóstico compõe a etapa de monitoramento que, apesar do nome e assim como consta no capítulo 2.2.4 desse artigo, é bom um ponto de partida para avaliar a maturidade da política de segurança da empresa. Com a aplicação do questionário de diagnóstico, resultou-se em

sugestões propondo a correção para os problemas encontrados que interfiram no andamento da conformidade. Para essa etapa utilizou-se um questionário adaptado da ISO/IEC 27001:2013.

O material é composto por 113 perguntas, com cada uma delas se avalia as medidas de segurança da empresa. Todas as perguntas são divididas em 22 categorias relacionando um caso específico ou outro presente entre os parágrafos e exigências da lei, a tabela 1 relaciona todas as perguntas bem como suas categorias.

Tabela 1: Questionário de diagnóstico

Perguntas	Medidas de Segurança e Privacidade/Categorias
A finalidade do tratamento é comunicada ao titular dos dados pessoais, mesmo no caso de execução de políticas públicas e competência legal, antes que as informações sejam coletadas ou usadas?	Abertura, Transparência e Notificação
No contrato, há a obrigação do operador de dados pessoais notificar o Controlador em caso de ocorrência de violação de dados pessoais?	Abertura, Transparência e Notificação
Os terceiros operadores de dados informaram no contrato sobre a utilização de subcontratos para processar dados pessoais?	Abertura, Transparência e Notificação
Os titulares de dados pessoais são notificados de alterações na forma de tratamento de dado	Abertura, Transparência e Notificação
São fornecidas aos titulares de dados pessoais informações claras e facilmente acessíveis sobre as políticas, procedimentos, práticas do controlador de dados pessoais em relação ao manuseio de dados pessoais (dados coletados, processamento efetuado, finalidade a ser alcançada com o processamento, com quem compartilha e a finalidade, capacidade de consentir compartilhamento específicos), como os dados são protegidos, dados de comunicação com o encarregado, entre outras informações de importância a transparência e publicidade?	Compliance com a Privacidade
Foi elaborada uma política de privacidade para o serviço?	Compliance com a Privacidade

Existe Relatório de Impacto à Proteção de Dados Pessoais, conforme previsto na Lei 13.709 de 14 de agosto de 2018, relacionado à solução de TIC?	Compliance com a Privacidade
O desenvolvimento dos sistemas tem como base os riscos e as medidas de segurança identificadas no RIPD (Relatório de Impacto de Proteção à Dados Pessoais)?	Compliance com a Privacidade
O desenvolvimento dos sistemas é orientado à proteção da privacidade dos dados pessoais (*Privacy by Design*)?	Compliance com a Privacidade
Os contratos firmados com os operadores de dados pessoais contêm cláusulas que asseguram o tratamento de dados pessoais conforme previsto pela Lei Geral de Proteção de Dados?	Compliance com a Privacidade
Há uma política ou norma de proteção de dados pessoais que aborde a finalidade da instituição perante o processamento de dados; a transparência com relação à coleta e processamento de dados pessoais; a estrutura estabelecida para a proteção de dados pessoais; regras para tomar decisões em questões de proteção de dados pessoais; critérios de aceitação de risco de privacidade; compromisso de satisfazer os requisitos aplicáveis de proteção à privacidade?	Compliance com a Privacidade
Os controles de proteção de dados pessoais são monitorados e auditados periodicamente para garantir que as operações que envolvam dados pessoais estejam em conformidade com as leis, regulamentos e termos contratuais aplicáveis?	Compliance com a Privacidade
É implementada e mantida uma estratégia abrangente de treinamento e conscientização, destinada a garantir que os envolvidos entendam suas responsabilidades e os procedimentos de proteção de dados pessoais?	Compliance com a Privacidade
A instituição monitora continuamente as ações de proteção de dados pessoais, a fim de determinar o progresso no cumprimento dos requisitos de conformidade com a proteção de dados pessoais e dos controles de proteção de dados pessoais, comparar o desempenho em toda a organização, identificar vulnerabilidades e lacunas na política e na implementação e identificar modelos de sucesso?	Compliance com a Privacidade

Existe Sistema de Gestão de segurança da Informação e já foi revisada para se adequar a medidas que objetivem a proteção de dados pessoais?	Compliance com a Privacidade
O Controlador obtém consentimento (LGPD, Art 7º, I) do titular de dados para o tratamento de dados pessoais que não se enquadre nas demais hipóteses previstas pelo art. 7º e 11 da LGPD?	Consentimento e Escolha
São implementados mecanismos e procedimentos para mitigar ataques de negação de serviço, tais como balanceamento de carga, proxy, firewall etc.?	Continuidade de Negócio
Existe um Plano de Continuidade de Negócio, que garanta o nível adequado de continuidade para a segurança da informação durante uma situação adversa?	Continuidade de Negócio
São realizados, em intervalos de tempo predefinidos, simulações e/ou testes planejados, levando-se em consideração as menores indisponibilidades e impactos possíveis nos processos de negócio, de forma que seja possível identificar falhas que venham a comprometer qualquer parte do processo de continuidade, com vistas a promover revisões e atualizações periódicas dos Planos relacionados?	Continuidade de Negócio
Há utilização de criptografia para a proteção dos dados sensíveis ou críticos armazenados em dispositivos móveis, mídias removíveis ou em banco de dados?	Controles Criptográficos
O compartilhamento ou transferência de dados pessoais é realizado por meio de um canal criptografado e recomendada pelos sites especializados de segurança	Controles Criptográficos
As permissões de acesso (incluir, consultar, alterar, excluir) dos usuários que executam a operação de processamento de dados pessoais se limitam ao mínimo necessário para realizar o processamento?	Controles de Acesso e Privacidade
O acesso para realizar as operações de tratamento de dados pessoais é provido ao número mínimo de indivíduos necessários para executar as operações de tratamento?	Controles de Acesso e Privacidade

Meios de autenticação forte são providos para o processamento dos dados pessoais, em especial os dados sensíveis (dados de saúde e demais dados previstos pelo art.5º, II da LGPD))?	Controles de Acesso e Privacidade
A organização controla por meio de um processo formal a concessão de direitos de acesso privilegiado para o processamento de dados?	Controles de Acesso e Privacidade
É exigida autorização prévia da chefia imediata para liberação das credenciais de acesso para o gerenciamento dos sistemas que suportam o serviço?	Controles de Acesso Lógico
O sistema em análise segue uma política de senha com definição de tamanho mínimo e formato?	Controles de Acesso Lógico
As informações das credenciais de acesso dos usuários estão gravadas em recursos de tecnologia da informação protegidos e sob a forma criptografada?	Controles de Acesso Lógico
As informações das credenciais de acesso dos usuários são transmitidas de forma protegida?	Controles de Acesso Lógico
Um mecanismo de recuperação de senha está implementado de forma a assegurar a recuperação da senha de maneira segura, sem fornecimento de senha por parte da aplicação, e que obrigue a alteração de senha do usuário no primeiro acesso?	Controles de Acesso Lógico
Uma análise crítica de direitos de acesso é realizada em um período previamente definido ou a qualquer momento depois de qualquer mudança nos direitos de usuários ou para verificação de incidentes de segurança?	Controles de Acesso Lógico
Há mecanismos para encerramento (expirar) de qualquer sessão cuja inatividade do usuário exceda um período predeterminado?	Controles de Acesso Lógico
Existem restrições de autenticação do usuário para acesso simultâneo a serviço(s), sistema(s) e/ou rede(s)?	Controles de Acesso Lógico
O sistema implementa restrições/limitadores para sucessivas tentativas de acesso mal sucedidas?	Controles de Acesso Lógico

As credenciais de acesso e logs são armazenadas separadamente dos dados das aplicações e dos sistemas?	Controles de Acesso Lógico
O local (Data Center/Departamentos) que processa as informações é restrito somente ao pessoal autorizado?	Controles de Segurança em Redes, Proteção Física e do Ambiente
O trabalho (Terceiros/Parceiros) nas áreas seguras é supervisionado?	Controles de Segurança em Redes, Proteção Física e do Ambiente
A rede corporativa é segmentada em domínios lógicos (limitando aos funcionários o acesso às redes e aos serviços de rede especificamente autorizados a usar), de acordo com cada rede local, atendendo às necessidades de fornecimento de serviço e proteção da rede corporativa?	Controles de Segurança em Redes, Proteção Física e do Ambiente
O acesso externo aos sistemas é provido de meios de segurança que protegem a confidencialidade e integridade dos dados trafegados, tais como o uso de VPN?	Controles de Segurança em Redes, Proteção Física e do Ambiente
Existem e são executados processos periódicos de cópias de segurança das configurações e sistemas operacionais dos switches e roteadores?	Controles de Segurança em Redes, Proteção Física e do Ambiente
Há uma política ou norma de backup que aborde os procedimentos operacionais que padronizam os processos de geração de cópias de segurança e recuperação de arquivos, assim como os processos de controle de acesso, armazenamento, movimentação e descarte das mídias que contêm cópias de segurança?	Cópia de Segurança
Está estabelecida a abrangência dos procedimentos de backup para cada tipo de informação (por exemplo, completa ou diferencial)?	Cópia de Segurança

É definido a abrangência dos testes de backup e sua periodicidade, de forma que os testes sejam planejados observando as dependências e relacionamentos entre sistemas, considerando inclusive os ambientes de continuidade de negócios, com o objetivo de minimizar a possibilidade de que a ausência de sincronismo entre os dados inviabilize ou dificulte sua recuperação?	Cópia de Segurança
As mídias que contêm cópias de segurança são armazenadas em uma localidade remota (“*offsite*”), a uma distância suficiente que garanta sua integridade e disponibilidade contra possíveis danos advindos de um desastre ocorrido no sítio primário?	Cópia de Segurança
O período de retenção das cópias de segurança e os requisitos de releitura são predefinidos, levando-se em consideração os requisitos de negócio, contratuais, regulamentares ou legais?	Cópia de Segurança
Existe uma frequência estabelecida para geração dos backups?	Cópia de Segurança
São realizadas cópias de segurança dos logs de acordo com períodos de retenção, que consideram os requisitos de negócio, contratuais, regulamentares ou legais?	Cópia de Segurança
Os dados pessoais armazenados/retidos possuem controles de integridade permitindo identificar se os dados foram alterados sem permissão?	Cópia de Segurança
Existe e é executado um processo formal de desenvolvimento de sistema seguro?	Desenvolvimento Seguro
As áreas de desenvolvimento, teste, homologação e produção são segregadas a fim de reduzir as possibilidades de modificação ou uso indevido dos recursos de processamento da informação, com controles de segurança adequados para cada ambiente?	Desenvolvimento Seguro
Em caso de desenvolvimento de sistemas de informação por terceiros, o proprietário do ativo da informação supervisiona o processo do planejamento até a implantação?	Desenvolvimento Seguro
Quando há a cópia dos dados de produção para os ambientes de desenvolvimento, teste e homologação, há autorização do proprietário do ativo de informação?	Desenvolvimento Seguro

Requisitos de segurança são identificados e considerados em todas as fases do projeto do sistema?	Desenvolvimento Seguro
Existem controles de versão para garantir a gestão dos códigos-fonte?	Desenvolvimento Seguro
As mensagens de erro do sistema não revelam detalhes da sua estrutura interna?	Desenvolvimento Seguro
É realizada análise estática e/ou análise dinâmica dos requisitos de segurança cibernética do sistema?	Desenvolvimento Seguro
A instituição revisa periodicamente as medidas de segurança aplicadas nos ativos que realizam o tratamento de dados pessoais (coleta, retenção, processamento, compartilhamento e eliminação)?	Desenvolvimento Seguro
Há mecanismos para monitoramento (*Zabbix/Nagios*) do uso dos recursos, de forma a atender as necessidades de capacidade futura e garantir o desempenho requerido das aplicações?	Gestão de Capacidade e Redundância
Há redundância dos recursos de processamento da informação suficiente para atender aos requisitos de disponibilidade previstos em contrato?	Gestão de Capacidade e Redundância
É realizado o controle de mudanças em atualizações de software e outros componentes das soluções de TIC?	Gestão de Mudanças
Mudanças são planejadas e testadas?	Gestão de Mudanças
Há uma avaliação de impactos potenciais, riscos e consequências, incluindo impactos de segurança cibernética, quando da identificação de necessidade de mudanças?	Gestão de Mudanças
As mudanças são comunicadas para todas as partes interessadas?	Gestão de Mudanças
Existe um prazo formalmente definido para o tratamento de vulnerabilidades técnicas relevantes identificadas?	Gestão de Mudanças

Há um inventário completo e atualizado dos ativos de informação, contendo o fornecedor, o número da versão, os dados pessoais processados, a classificação dos dados pessoais (sensíveis ou apenas dados pessoais), quais softwares estão instalados e em quais sistemas, e a(s) pessoa(s) na organização responsável(s) pelos ativos?	Gestão de Riscos
Há um processo de análise e monitoramento de vulnerabilidades?	Gestão de Riscos
É realizada periodicamente uma análise/avaliação de riscos da arquitetura da Solução de TIC, indicando os eventos de risco e seus respectivos níveis de risco ao qual o sistema está exposto, baseada em prévia análise de vulnerabilidades dos ativos que compõem a Solução de TIC?	Gestão de Riscos
Os recursos de segurança da informação e de tecnologia da informação encontram-se em versões seguras, estáveis e atualizadas?	Gestão de Riscos
O responsável pelo sistema acompanha junto aos fabricantes o período de obsolescência do produto, para evitar que os componentes se tornem expostos a vulnerabilidades sem correção?	Gestão de Riscos
Os dados pessoais encontram-se classificados em sensíveis e não sensíveis, incluindo categorias de informações pessoais de saúde, informações pessoais financeiras, entre outras?	Legitimidade e Especificação de Propósito
Há um inventário completo e atualizado dos dados pessoais, contendo os agentes de tratamento (controlador e operador), encarregado, descrição do fluxo de tratamento dos dados pessoais (como são coletados, armazenados, processados, retidos e eliminados), abrangência da área geográfica do tratamento (nacional, estadual, municipal), finalidade do tratamento dos dados pessoais, categoria dos dados pessoais (identificação pessoal, financeiros, características pessoais, outros), categoria de dados sensíveis, dados pessoais compartilhados e transferência internacional?	Legitimidade e Especificação de Propósito
O tratamento de dados pessoais é realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público? (embasamento legal)	Legitimidade e Especificação de Propósito

As transferências internacionais de dados pessoais são realizadas de acordo com o disposto pelo art. 33 da Lei 13.709/2018 (LGPD)?	Legitimidade e Especificação de Propósito
Os dados coletados limitam-se ao mínimo necessário para atendimento da finalidade do tratamento?	Limitação da Coleta
É realizada uma análise periódica sobre os dados coletados, se eles continuam limitados ao mínimo necessário para o atendimento a finalidade?	Limitação da Coleta
Os dados pessoais utilizados em ambiente de TDH (teste, desenvolvimento e homologação) passaram por um processo de anonimização?	Limitação da Coleta
A instituição utiliza técnicas ou métodos apropriados para garantir exclusão ou destruição segura de dados pessoais (incluindo originais, cópias e registros arquivados), de modo a impedir sua recuperação?	Limitação da Coleta
Ao fornecer a base de informações para órgãos de pesquisa, os dados pessoais são anonimizados ou pseudoanonimizados?	Limitação da Coleta
No processamento de dados, é utilizado o mínimo necessário de dados pessoais para atingir a finalidade pretendida?	Minimização dos Dados
É avaliada a necessidade de permitir que operadores e administradores de banco de dados usem linguagens de consulta, que habilitam recuperação maciça automatizada de bases de dados que contêm dados pessoais?	Minimização dos Dados
A instituição permite aos titulares dos dados pessoais, quando permitido pela legislação aplicável, a capacidade de acessar e revisar seus dados pessoais para elevar a integridade e precisão das informações?	Participação Individual e Acesso
Há um canal de comunicação ativo, seguro e autenticado para o recebimento de reclamações e manter um ponto de contato para receber e responder a reclamações, preocupações ou perguntas dos titulares sobre o tratamento de dados pessoais realizados pela instituição?	Participação Individual e Acesso
A instituição implementa processos para que o tratamento dos dados pessoais seja preciso, completo, atualizado, adequado e relevante para a finalidade de uso?	Precisão e qualidade

A instituição implementa medidas que garantam e maximizem a precisão dos dados pessoais coletados, antes de qualquer armazenamento ou processamento de dados pessoais?	Precisão e qualidade
O log registra identificação do usuário, incluindo administrador e acessos privilegiados?	Registro de Eventos, Rastreabilidade e Salvaguarda de Logs
O log registra endereço IP ou outro atributo que permita a identificação de onde o usuário efetuou o acesso?	Registro de Eventos, Rastreabilidade e Salvaguarda de Logs
O log registra as ações executadas pelos usuários?	Registro de Eventos, Rastreabilidade e Salvaguarda de Logs
O log registra data e hora do evento com alguma fonte de tempo sincronizada?	Registro de Eventos, Rastreabilidade e Salvaguarda de Logs
Os logs gerados são protegidos, quando da geração, contra edição e exclusão?	Registro de Eventos, Rastreabilidade e Salvaguarda de Logs
Os logs são protegidos contra o acesso indevido?	Registro de Eventos, Rastreabilidade e Salvaguarda de Logs
As operações de processamento realizadas com dados pessoais são registradas de modo a identificar a operação realizada, quem realizou, data e hora?	Registro de Eventos, Rastreabilidade e Salvaguarda de Logs
Há uma matriz de responsabilidades com atribuição pela segurança da informação na organização (Corpo Diretivo/Gerência Executiva), identificação dos gestores de serviços com dados pessoais (Departamentos), pela proteção de dados (Encarregado), operadores de tratamento de dados (Colaboradores/Funções), de forma a evidenciar a segregação de funções e assegurar que colaboradores e partes externas entendam suas responsabilidades (Treinamentos)?	Responsabilização
No compartilhamento de dados com terceiro, o operador ou órgãos públicos, são documentadas as informações de limitação do tratamento dos dados pessoais ao mínimo necessário para atendimento do fornecimento do serviço e dispositivo legal?	Responsabilização

Acordos de confidencialidade, termos de responsabilidade, termos de sigilo são assinados com os órgãos e operadores de dados pessoais? É importante que os termos e acordos informem a respeito dos itens a seguir, mas a eles não se limitem: tipos de tratamento de dados pessoais a serem realizados por quem irá receber os dados; ações requeridas quando do encerramento do compartilhamento, como destruição dos dados, responsabilidade e ações dos signatários para evitar a divulgação não autorizada dos dados pessoais; base legal para o compartilhamento; direito de auditar e monitorar as atividades que envolvem os dados pessoais; processo para notificar ou relatar vazamentos; violações ou divulgações não autorizadas dos dados pessoais; ações a serem tomadas diante da violação do acordo; e outras medidas possíveis.	Responsabilização
Os contratos firmados com os operadores contêm cláusulas que contemplam, não se limitando a: uma declaração adequada sobre a escala, natureza e finalidade do processamento contratado; relatar casos de violação de dados, processamento não autorizado ou outro não cumprimento dos termos e condições contratuais; medidas aplicáveis na rescisão do contrato, especialmente no que diz respeito à exclusão segura de dados pessoais; impedimento de tratamento de dados pessoais por subcontratados, exceto por aprovação do controlador?	Responsabilização
O compartilhamento e a transferência de dados pessoais com operadores ou órgãos públicos são registrados, incluindo quais dados pessoais foram divulgados, a quem, a que horas e com que finalidade?	Responsabilização
Existe uma equipe de detecção, tratamento e resposta a incidentes de segurança cibernética (CSIRT)?	Resposta a Incidente
Há um sistema para monitoramento de aplicações, alertas e vulnerabilidades utilizado para auxiliar na detecção e tratamento de incidentes de segurança cibernética (IPS, IDS etc.)?	Resposta a Incidente
O plano de comunicação foi atualizado para incluir os contatos que devem ser notificados, caso haja uma violação de privacidade, ou para reportar detalhes de processamento, como contatos com a autoridade de proteção de dados e/ou grupos diretamente relacionados?	Resposta a Incidente

Nos casos em que seja inviável preservar as mídias de armazenamento em razão da necessidade de pronto restabelecimento do serviço afetado, o agente responsável pelo CSIRT coleta e armazena cópia dos arquivos afetados pelo incidente, tais como: logs, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original, bem como os "metadados" desses arquivos, como data, hora de criação e permissões; registrando em relatório a impossibilidade de preservar as mídias afetadas e listando todos os procedimentos adotados?	Resposta a Incidente
Os arquivos coletados como evidências são gravados em conjunto com o arquivo com a lista dos resumos criptográficos?	Resposta a Incidente
Os ativos de informação estão configurados de forma a registrar todos os eventos relevantes de segurança da informação, contendo, pelo menos, a identificação inequívoca do usuário, a natureza do evento, a data, hora e fuso horário, o identificador do ativo de informação, as coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento?	Resposta a Incidente
Existe um canal apropriado para notificar os incidentes de segurança da informação de forma rápida?	Resposta a Incidente
Existem formalmente e são executados procedimentos específicos para resposta aos incidentes, contemplando: a definição de incidente; o escopo da resposta; quando e por quem as autoridades devem ser contatadas; papéis, responsabilidades e autoridades; avaliação de impacto do incidente; medidas para reduzir a probabilidade e mitigar o impacto do incidente; descrição da natureza dos dados pessoais afetados; as informações sobre os titulares de dados pessoais envolvidos; procedimentos para determinar se um aviso para indivíduos afetados e outras entidades designadas (por exemplo, órgãos reguladores) é necessário?	Resposta a Incidente
O servidor da aplicação fornece opções de protocolos criptográficos para conexão em versões seguras, estáveis e atualizadas?	Segurança Web
O servidor da aplicação tem configurado o cabeçalho HTTP com *X-XSS-Protection* para evitar que usuários de navegadores antigos sejam vulneráveis a ataques de *Cross-site Scripting (XSS)*?	Segurança Web

O servidor da aplicação tem configurado o cabeçalho HTTP com *X-Frame-Options* para evitar que usuários caiam em ataques de *clickjacking*?	Segurança Web
O servidor da aplicação tem configurado o cabeçalho HTTP com *HTTP Strict-TransportSecurity* (HSTS) para garantir que todo o tráfego de dados ocorra criptografado?	Segurança Web
O servidor da aplicação implementa políticas (*Content Security Policy* (CSP)) que validam a renderização da página e protegem contra ataques de injeção de conteúdo como *Cross-Site Scripting* (XSS)?	Segurança Web
O servidor da aplicação implementa o *X-ContentType-Options* para evitar que navegadores como Internet Explorer e Chrome interpretem o conteúdo da página e execute o dado como código?	Segurança Web
Os cookies da aplicação são enviados para o usuário apenas através de conexões criptografadas (*flag SECURE*)?	Segurança Web
A aplicação está configurada para que os cookies não possam ser acessíveis via comando *JavaScript*, evitando assim ataques *cross-site scripting* (XSS) (*flag HTTPOnly*)?	Segurança Web
O servidor da aplicação está configurado com o cabeçalho *Subresource Integrity* (SRI) para proteger contra invasores que modifiquem o conteúdo de bibliotecas *JavaScript* hospedadas em redes de entrega de conteúdo (CDNs)?	Segurança Web

Fonte: Adaptado da ISO/IEC 27001:2013

Na categoria “Abertura, Transparência e Notificação” busca a informação se o titular é avisado da finalidade da coleta e tratamento dos dados e qualquer alteração da forma de tratamento de dados, também pergunta se terceiros operadores de dados têm transparência no seu contrato. Além disso, as empresas devem deixar claro e assegurar que o titular dos dados tem total acesso aos seus dados, informações que são diagnosticadas na categoria “Participação Individual e Acesso”.

Outras perguntas a respeito da coleta e tratamento de dados são divididas entre “Legitimidade e Especificação de Propósito” que pergunta sobre a procedência da classificação de dados e se há um embasamento legal sobre o tratamento

realizado, “Limitação da Coleta” e “Minimização de Dados” corresponde ao critério de a instituição ter o mínimo necessário para realizar as operações e por último “Precisão e Qualidade” que pergunta se os dados coletados são exatos e relevantes para o cumprimento da finalidade do tratamento.

Além disso no segmento “Consentimento e Escolha” possui apenas uma pergunta, porém de extrema importância pois é com ela que se analisa sobre a obtenção do consentimento do titular, desde que não se enquadre nas demais hipóteses previstas pelo art. 7º e 11º da LGPD.

“Compliance com a Privacidade” há perguntas que se busca saber a procedência da política de privacidade da empresa e se atende a legislação de proteção de dados. Em termos de privacidade, a instituição também deve limitar acessos indevidos às operações de tratamento de dados pessoais, oferecer um meio seguro para as comunicações e armazenamento de registros e usar o recurso da criptografia, esses casos ficam por parte de “Controles de Acesso e Privacidade” e “Controles Criptográficos”.

Com a análise das perguntas de “Registro de Eventos, Rastreabilidade e Salvaguarda de Logs” determina se a empresa faz registro de eventos com atributos de rastreabilidade e proteção de alteração e acessos indevidos. Da mesma forma que “Controles de Acesso Lógico” e “Controles de Segurança em Redes, Proteção Física e do Ambiente” busca saber se limitam os acessos indevidos ao sistema e evitam acessos indevidos às estruturas internas.

Seja qualquer eventualidade as operações da instituição devem continuar na ativa e a elaboração de uma boa política de segurança é de extrema importância em casos como esses, as perguntas que avaliam isso estão divididas em três seções: “Continuidade de Negócio”, “Cópia de Segurança” e “Resposta a Incidente”. Esse último se busca conhecimento sobre as ações da empresa com relação à realização da coleta, da preservação de evidências, do tratamento e da resposta à incidentes de segurança. Além do que, a empresa deve manter a disponibilidade do serviço, caso que é analisado em “Gestão de Capacidade e Redundância”.

A “Gestão de Mudanças” prevê o acompanhamento das mudanças, comunicação aos interessados e identificação de potenciais riscos. Em “Gestão de Riscos” procura-se entender se a empresa está pronta para a identificação, avaliação, gerenciamento e monitoramento dos riscos identificados.

A instituição deve protocolar medidas que atenda os critérios de segurança da informação, desde a concepção do produto. Por isso as questões de “Desenvolvimento Seguro” buscam-se entender se existe e é executado um processo formal de desenvolvimento de sistema seguro e se as áreas de desenvolvimento, teste, homologação e produção são segregadas a fim de reduzir as possibilidades de modificação ou uso indevido dos recursos de processamento da informação, com controles de segurança adequados para cada ambiente, além de outras perguntas que ajudam a analisar esse critério.

No quesito de “Segurança Web” consta informações sobre a criptografia nos protocolos de segurança no servidor da aplicação, a configuração de segurança nos cabeçalhos HTTP para evitar que usuários de navegadores antigos sejam vulneráveis a ataques, em resumo, busca-se saber se a empresa eleva os níveis de segurança nos serviços de acessos eletrônicos.

Por fim, as perguntas da categoria “Responsabilização” buscam saber se adotam medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

3.2.1 Avaliação da política de segurança

Diferente da pesquisa de validação de problema em que cada pergunta foi respondida com “sim” ou “não”, no caso do questionário de diagnóstico cada questão foi respondida com uma nota de 0 a 5 sendo esse o grau de implantação da tal medida atribuída à pergunta, com essas notas realizou-se os cálculos dos índices de todas as categorias como já mencionadas.

3.2.2 Análise e recomendações

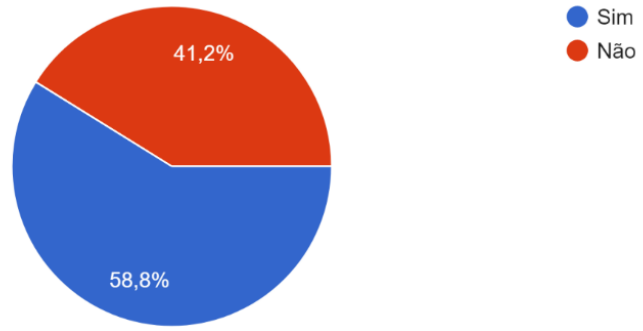
Para a empresa dar início às próximas etapas, puderam contar com a análise feita através da atividade. Essa etapa se constituiu em revisar todas as perguntas respondidas e para cada uma que apresentou uma preocupação maior ou algum problema foi relacionada recomendações com base em normas ISO para ajudar as empresas a rever sua política de segurança da informação.

4 RESULTADOS E DISCUSSÕES

4.1 PESQUISA GERAL DE CONFORMIDADE E VALIDAÇÃO DO PROBLEMA

Obteve-se respostas de 17 micro, pequenas e médias empresas de vários ramos, apesar de não alcançar respostas de outras 13 empresas contatadas os dados mostram-se suficientes para a análise da pesquisa. A primeira pergunta busca-se saber se a empresa possui controle contra riscos de segurança da informação, percebe-se que 41,2% ainda não possuem como mostra na figura 4.

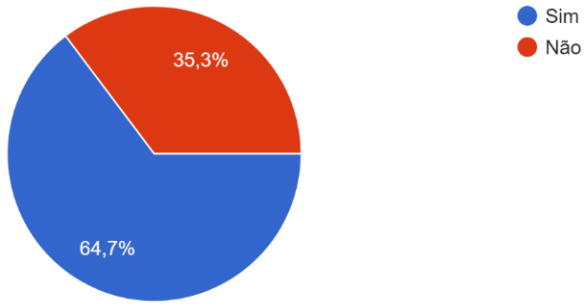
Figura 4: Primeira pergunta



Fonte: Do autor

A pergunta seguinte está relacionada à segurança de controle de acesso, item extremamente importante pois visa o não acesso de intrusos ou de pessoas não autorizadas, com a ajuda da figura 5 entende-se que nesse caso há uma situação mais favorável apesar das respostas negativas somarem 35,3%.

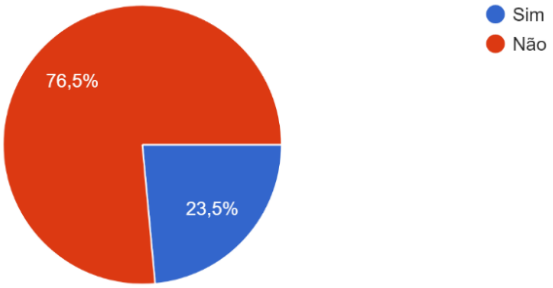
Figura 5: Controle de acesso



Fonte: Do autor

Uma boa política de segurança da informação é benéfica para o negócio no geral, infelizmente nem todas as empresas têm uma política que supri as necessidades do mercado, nessa pesquisa esse cenário se encontra na grande maioria como pode-se notar na figura 6.

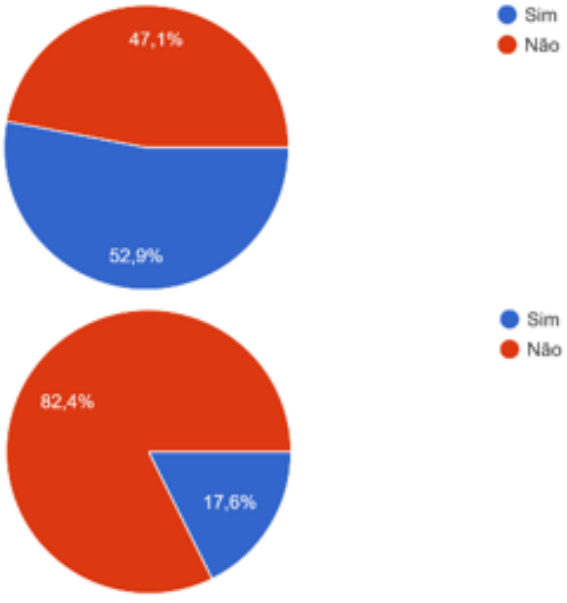
Figura 6: Política de segurança para necessidade do negócio



Fonte: Do autor

É importante que as empresas tenham líderes que promovam uma cultura positiva e tenham conversas sobre a proteção de dados, nesse cenário obteve-se pouco mais de 52% de respostas positivas, como nota-se na figura 7. Porém um dado negativo visível na mesma figura é de que 82,4% das empresas não promovem treinamento de conscientização sobre segurança da informação.

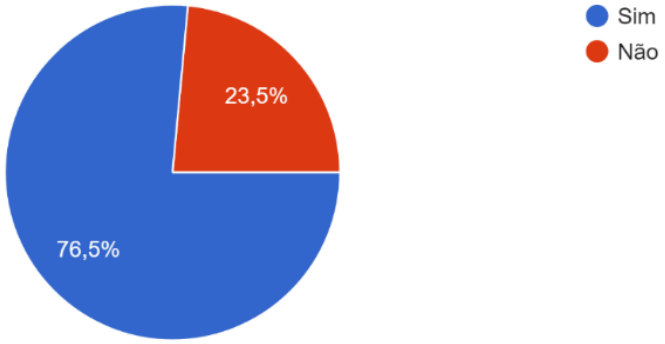
Figura 7: Conscientização e treinamento



Fonte: Do autor

Podem ocorrer desastres tanto físicos quanto digitais e as empresas devem estar preparadas sob qualquer eventualidade e os dados armazenados podem ser os mais afetados, comprometendo todo o trabalho da instituição. Uma ferramenta valiosa para esse cenário é o backup, com ele é possível retomar o controle das atividades sem maiores problemas, o problema é que pouco mais de 20% das repostas obtiveram resultados negativo com relação a política de backup como pode-se analisar na figura 8.

Figura 8: Backup

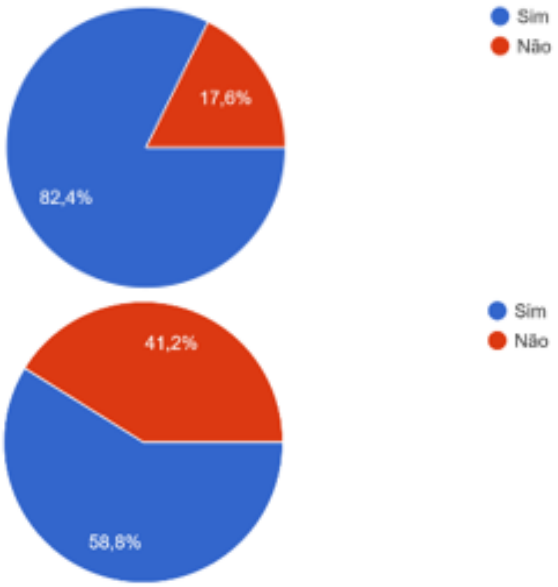


Fonte: Do autor

Continuando essa linha de desastres, como perda de dados, é incontestável a utilização de firewall e anti-malware, sendo essas ferramentas de proteção digitais que combate a intrusão e fazem a remoção de vírus nos computadores da empresa. A exemplo da pergunta da figura 8 sobre backup, uma forma de perder ou não ter mais acesso aos dados armazenados é através da intrusão de ransomware que sequestra os dados da empresa e é liberado apenas se pago um valor pedido pelo hacker, por isso destaca-se a importância de backup, firewall e anti-malware com gestão centralizada.

A pesquisa mostra dados preocupantes quanto a segurança com relação a dados e computação, como mostra na figura 9, 17,6% afirmam de a empresa não possuir firewall para proteção enquanto apenas 58,8% utilizam anti-malware com gestão centralizada.

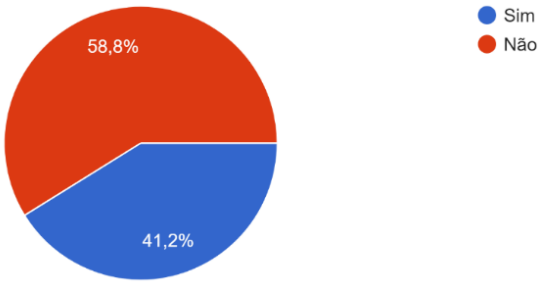
Figura 9: firewall e anti-malware



Fonte: Do autor

A seguinte pergunta destaca, não os computadores da empresa, mas o equipamento do colaborador. Entende-se que se o colaborador tem acesso aos dados da empresa ele deve ser gerenciado com segurança, seja por proteção digital, com firewall e anti-malware, seja por conduta profissional, porém mais da metade não gerenciam com segurança seus colaboradores, como detalhado na figura 10.

Figura 10: Gerenciamento dos colaboradores

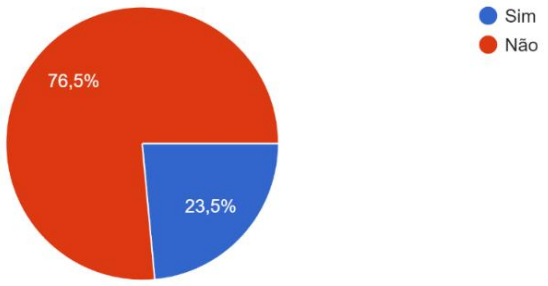


Fonte: Do autor

A última pergunta da pesquisa retrata uma das exigências da lei e de importante discussão, sobre a empresa usar os dados para outras finalidades além do que foi proposto. Ainda que não tenha uma pergunta seguida dessa que se busca saber se a empresa comunica o titular dos dados, é um dado interessante de ser

analisado, pois caso não haja a comunicação, os 23,5% terão problemas com a conformidade e a fiscalização, como pode-se notar na figura 11.

Figura 11: Finalidade



Fonte: Do autor

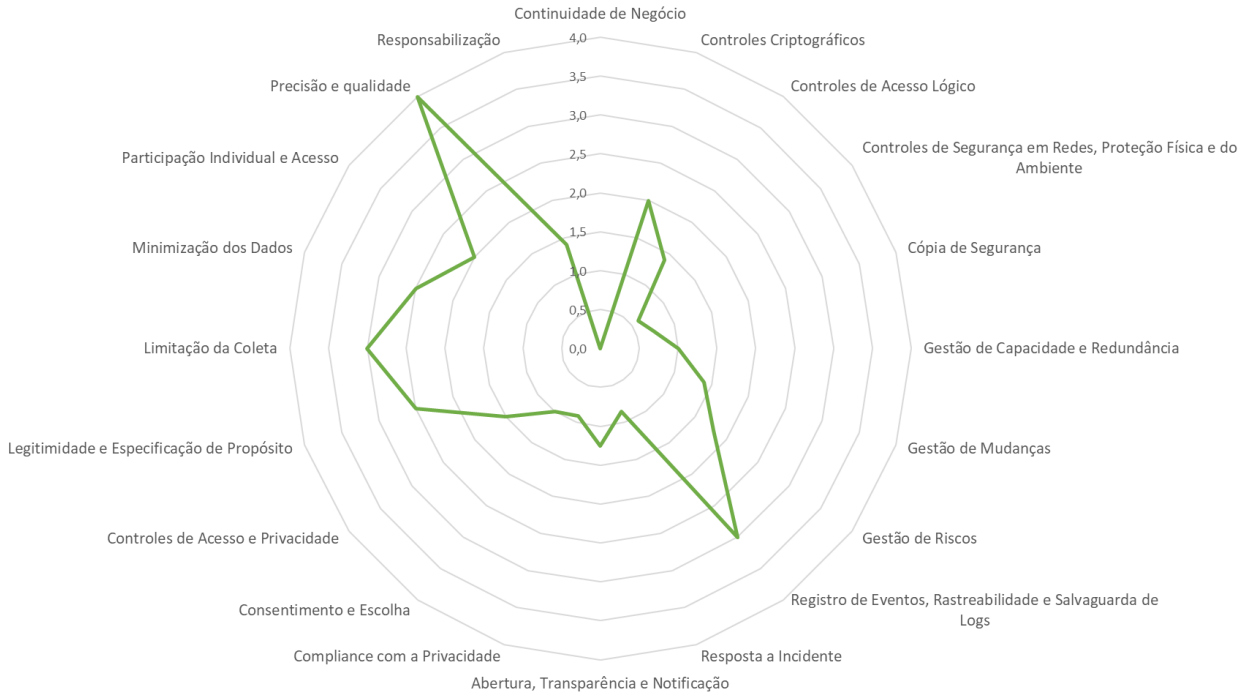
Poucas empresas demonstraram interesse ou deixaram o contato para a realização do diagnóstico, os e-mails recolhidos na última seção de pesquisa foram suficientes para a identificação de uma empresa apta para a realização da etapa seguinte.

4.2 DIAGNÓSTICO DE CONFORMIDADE EM UMA EMPRESA

Após a análise das repostas concedidas na pesquisa de conformidade, realizou-se o procedimento em conjunto com a Padilha Contabilidade, uma empresa de Forquilhinha que começou seus trabalhos em 1990, atualmente abrange 6 municípios da região sul de Santa Catarina, atendendo o equivalente a 100 empresas por mês além de um número variado de pessoas físicas. A empresa realiza serviços que se enquadram na área de Ciências Contábeis, como constituição de empresas, ações trabalhistas, escrituração fiscal e legalização de empresas, tendo contato diário com dados tanto de pessoas físicas como jurídicas.

Realizou-se o contato para troca de informações e conhecimentos, tanto sobre a empresa como sobre a LGPD, e feito o diagnóstico de forma presencial e por meio de troca de mensagens chegando ao resultado mostrado na figura 12, ressaltando que a Padilha Contabilidade concedeu a devida autorização para a utilização de seus dados para a pesquisa desse presente artigo.

Figura 12: Gráfico gerado com os índices calculados



Fonte: Do autor

Com a análise de todo o questionário respondido possibilitou traçar uma recomendação para que pudessem estudar as necessidades para a conformidade. Com relação aos dados coletados, o cliente já tem as informações sobre a coleta já no contrato, o que ainda falta é estabelecer um contato direto e seguro com o titular de dados para comunicação de violação ou mudança nos termos, assim como devem melhorar o fornecimento de informações, a ISO/IEC 29151:2017 deve ajudá-los a complementar a política de privacidade que irão implementar.

Em paralelo a isso, a empresa deve melhorar sua segurança interna e pode recorrer a ajuda da ISO/IEC 27002:2013 e ISO/IEC 27701:2019 com o objetivo de desenvolver um sistema de gestão de segurança da informação e privacidade de dados.

Das mudanças, inclui fazer uso da criptografia em documentos e meios de comunicação que dificultará acesso em caso de roubo de dados, assim como encontrar um meio para troca de informações de forma segura e rever a política de controle de acesso, já que todos dentro da empresa possui acesso a todos os dados, sendo que os colaboradores terão acesso à apenas o mínimo necessário para realizar seu serviço tendo um controle adequado.

Ainda sobre os colaboradores, recomendou-se que tenham treinamento adequado de conscientização sobre segurança da informação e que a alta gestão promova uma cultura positiva de conformidade de proteção de dados.

A empresa deve redefinir sua política de backup, poucos documentos se encontram em nuvem e muitos não são digitalizados, tendo em vista que podem ocorrer desastres tanto em meio físico quanto digital, recomendou-se procurar um serviço em nuvem com alta disponibilidade e com segurança na conexão.

Deve também contratar um serviço de firewall e anti-malware para segurança dos computadores locais, assim como recomendou-se gerenciar a segurança de dispositivos de colaboradores em trabalhos remotos e/ou incentivá-los na segurança de seus dispositivos pessoais, se for o caso. Além de a empresa ter de traçar um plano para casos de desastres ou qualquer eventualidade negativa, como perda de dados, intrusão de ransomware ou perda de documentos físicos, é importante que tenha planos para continuar com seus trabalhos ou ajudá-los em recursos respondendo a uma eventual infração.

Assim como mostra na figura 12, o cenário de “Continuidade de Negócio” obteve o índice mais baixo entre todos. Isso porque usam firewall gratuito ou primário do próprio sistema operacional, sendo que a contratação de um serviço de segurança seja a escolha mais assertiva, não há um plano para continuidade de negócio com um nível adequado de continuidade para a segurança da informação e não é realizado testes com a finalidade de identificar falhas. Eventualmente recomendou-se buscar referência na ISO/IEC 27002:2013 nos capítulos 13.1.2 e 17.1 e a ISO 22301, porém essa recomendação sujeita-se ao porte da empresa e cabe segundas opiniões no tratamento dessa questão, visto a demanda de mercado as empresas devem estar em conformidade em relação a sua realidade.

Outras informações, recomendações e referências foram abordadas para ajudá-los na conformidade, ressalta-se que algumas perguntas foram descartadas conforme a realidade da empresa, valendo da informação de não ser desenvolvedora de sistemas ou mesmo ter uma aplicação em ambiente online para utilização dos clientes.

6 CONSIDERAÇÕES FINAIS

É indiscutível a importância da LGPD dado os últimos anos, visto que tem crescido o número de notícias sobre dados vazados de milhões de brasileiros assim como tem crescido o número de empresas que vendem dados sem que o titular saiba. A lei é de extrema importância para proteger pessoas físicas, com o desenrolar do presente trabalho percebe-se isso.

De modo geral, com a pesquisa obteve-se um amplo embasamento dos problemas que as empresas têm com relação à segurança de dados pessoais e o grau de maturidade à LGPD constatando alguns dados preocupantes, assim como ajudou a buscar uma empresa que esteja com certo grau de desconformidade.

O diagnóstico mostra-se um item essencial para ter conhecimento do quanto a empresa está em conformidade com a LGPD e é também uma ferramenta que deve ser consultada regularmente.

Com relação ao trabalho feito em conjunto com a empresa, foi realizada com certas dificuldades, porém com bons resultados, apesar de ser um processo essencialmente presencial pois demanda de tempo de conversa em reunião com a alta gestão, para conhecimento da empresa e seus processos, além de ter de passar o conhecimento sobre a LGPD para todos, a atividade transcorreu satisfatoriamente de forma que não ocorreram problemas maiores

O material para diagnóstico se mostrou eficiente em primeiro momento, tendo ponto fraco ser construído em planilhas, demandando tempo para organização sendo confuso em certos aspectos. Porém, mostra um bom potencial caso seja feito um questionário mais elaborado e organizado ou então uma aplicação para essas finalidades.

De certo modo, para trabalhos futuros, há a possibilidade de, além de desenvolver o diagnóstico e preparar recomendações para próximas etapas, desenvolver em conjunto um plano básico de continuidade das atividades e realizar um roteiro com as etapas a serem conquistadas, podendo inclusive acompanhar e relatar os primeiros passos que foram tomados, dessa forma aproveita-se para aplicar boa parte do conhecimento adquirido através do diagnóstico.

Obteve-se bons resultados com a atividade no sentido de encontrar e detalhar o que a empresa deve melhorar para ter uma boa política de segurança da

informação. Com as recomendações passadas e com a ajuda de um profissional na área ou uma pessoa capacitada que tenha conhecimento no processo de conformidade, certamente a Padilha Contabilidade estará dentro dos conformes da Lei Geral de Proteção de Dados.

REFERÊNCIAS

ABNT. ABNT NBR ISO/IEC 27701: 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. Brasil. 2019.

ABNT. ABNT NBR ISO/IEC 27001: Tecnologia da informação — **Técnicas de segurança — Sistemas de gestão de segurança da informação** — Requisitos. Brasil. 2006

ABNT. ABNT NBR ISO/IEC 27002: Tecnologia da informação — **Técnicas de segurança — Código de prática para controles de segurança da informação**. Brasil. 2013.

ABNT. ABNT NBR ISO/IEC 29151: Tecnologia da informação - **Técnicas de segurança - Código de prática para proteção de dados pessoais**. Brasil. 2017.

ABNT. ABNT NBR ISO/IEC 22301: Segurança e resiliência — **Sistema de gestão de continuidade de negócios — Requisitos**. Brasil. 2019.

ALBRECHT, Jan Philipp. **How the GDPR Will Change the World**. EDPL, n. 3, p. 287-289, 1 jan. 2016.

BRASIL. [Constituição (1988)]. **CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988**. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 23 mar. 2021.

BRASIL. **LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.** Brasília, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 23 mar. 2021.

BRASIL. **Guia de Elaboração de Programa de Governança em Privacidade**. 2020. Disponível em: <https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaProgramaGovernanaemPrivacidade.pdf>. Acesso em: 23 mar. 2021.

BURROWS, Leah. To be let alone: Brandeis foresaw privacy problems: What would the privacy-law champion make of surveillance programs like PRISM?. **BrandeisNOW**, 24 jul. 2013. Disponível em: <https://www.brandeis.edu/now/2013/july/privacy.html>. Acesso em: 23 mar. 2021.

EU. Regulations: **REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016**. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 23 mar. 2021.

JOHNSON, Eric. Why Europeans care more about data privacy than Americans: At least according to Europe's Commissioner for Competition Margrethe Vestager. **Recode**, 20 set. 2016. Disponível em: <https://www.vox.com/2016/9/20/12982524/europe-data-privacy-regulation-margrethe-vestager-recode-podcast>. Acesso em: 23 mar. 2021.

HOLVAST, Jan. History of Privacy In: The History of Information Security. **A Comprehensive Handbook**. p. 737-769, 2007. DOI <https://doi.org/10.1016/B978-044451608-4/50028-6>. Disponível em: <https://link.springer.com/content/pdf/10.1007%2F978-3-642-03315-5_2.pdf>. Acesso em: 23 mar. 2021.

ONU. **Universal Declaration of Human Rights** 1948. Disponível em: <https://www.un.org/sites/un2.un.org/files/udhr.pdf> Acesso em: 23 mar. 2021.

POHLMANN, Sérgio. **LGPD Ninja**: Entendendo e Implementando a Lei Geral de Proteção de Dados nas empresas. 1. ed. Novo Friburgo: Editora Fross, 2019. 240 p. v. 1. ISBN 9781089345886.

RIVELLI, Fabio. **Aplicação da Lei Geral de Proteção de Dados**. LBCA, 21 set. 2020. Disponível em: <https://lbca.com.br/aplicacao-da-lei-geral-de-protecao-de-dados-lgpd/>. Acesso em: 23 mar. 2021.

SILVA, Rogério Hermínio Da. **FLGPD: FRAMEWORK PARA AVALIAÇÃO DE CONFORMIDADE COM A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS.** Araranguá. 2021. Disponível em: < https://repositorio.ufsc.br/handle/123456789/222071>. Acesso em: 20 abr. 2021.