CHECKLIST DE CONFORMIDADE PARA ADEQUAÇÃO A LEI GERAL DE PROTEÇÃO DE DADOS

COMPLIANCE CHECKLIST FOR FITNESS TO GENERAL DATA PROTECTION LAW

Marcos Cavalcante Ribeiro[1]
Dr. Leonardo Gardini[2]
Dra. Mirley Nadila[3]

RESUMO
Os negócios atuantes no Brasil vem buscando se adequar a LGPD – Lei Geral de Proteção de Dados – o mais rápido possível. Diante das intensas discussões para aplicação de medidas este trabalho visa apresentar um modelo de auditoria para verificação de conformidades com o intuito de ajudar os interessados a testarem sua fiscalização interna. O *checklist* apresentado peça ICA – *Information Commissioner's Office* – foi utilizada na lei de proteção de dados da Europa com questionamentos de verificação de atividades que visam a conformidade. Baseado neste item, foram criadas perguntas semelhantes mas voltadas para a LGPD. Com a alimentação destes dados que representam um determinado cenário, um resultado final é apresentado após análise quantitativa de itens que correspondem positivamente à nova lei.

Palavras-chave:1. LGPD. 2. GDPR. 3. Privacidade 4. Proteção de dados 5. Conformidade em segurança.

ABSTRACT
Businesses operating in Brazil have been seeking to adapt the LGPD – General Data Protection Act – as soon as possible. In the face of intense discussions on the application of measures, this paper aims to present an audit model to verify compliance in order to help stakeholders test their internal supervision. The checklist submitted by ICA – Information Commissioner's Office – was used in the European Data Protection Act with compliance verification activity questions. Based on this item, similar but LGPD questions were created. With the feeding of these data that represent a certain scenario, a final result is presented after quantitative analysis of items that correspond positively to the new law.

Keywords: *1. LGPD. 2. GDPR. 3. Privacy 4. Data Protection 5. Security Compliance. 6. ANPD.*

[1] Estudante, Graduado em Redes de Computadores pela universidade Federal do Ceará
[2]
[3]Pedagoga, Mestre e Doutoranda em Educação e Tecnologias pela Universidade Federal do Ceará

1 INTRODUÇÃO

O homem vive uma intensa globalização, por meios de dispositivos que estão em crescente aumento visto que tudo está conectado a Internet por meio de tecnologias que se comunicam em rede. Isto é comprovado pelo instituto LACNIC (2017), que afirma que os 4 milhões de endereços Ipv4 estarão esgotados até o início de 2021 e por ARBACHE (2015), que expõe o aumento de usuários de internet nos últimos anos. Esta necessidade ocorre porque o meio digital está a cada dia sofrendo inovações com tecnologias que prometem melhorias de serviço como *Machine learning, IoT, Big Data* entre outras. Estas tecnologias impactam em como desenvolver e aplicar estas melhorias para os projetos que movem empresas de economia privada, pública ou mista.

No entanto, tanto crescimento não possuía regimento eficaz da lei quanto às informações pessoais que nelas trafegavam e ao tratamento da privacidade, que era facilmente violada sem conceder às empresas responsabilidades pela forma como tratavam os dados. Foi o caso do banco Inter que foi acusado de permitir a visualização de dados como nome completo, endereço de e-mail e CPF na Internet. Esta falha tornou 1,45 milhão de usuários expostos pelo período de um ano, como explica o portal de notícias Tecnoblog (2017) baseado numa denúncia anônima. Como não existia lei sobre privacidade destes dados nada foi feito e a empresa consertou o problema sem se responsabilizar.

Este tipo de situação tem incomodado especialistas e um movimento surgiu para questionar esta responsabilidade sobre as informações que eram guardadas nas empresas. O primeiro a tomar uma posição foi o Conselho da União Europeia, que obrigou empresas a protegerem mais os dados pessoais quanto ao quesito privacidade por meio da lei europeia 2016/679 conhecida como GDPR – *General Data Protection Regulation*. Segundo *Wall Street Journal* (2019), a multa mais alta já aplicada chega em 5 bilhões de dólares para a empresa Facebook e segundo JOTA (2019), entre o período de 2018 e 2019 obteve-se mais de 40 mil notificações sobre ameaças ou incidentes.

Para resolver este problema na GDPR – que já está em vigor desde 2015 – foram elaborados vários planos de *checklist* chamados de IAPD que estudam o quão a empresa está conforme em uma auditoria. Existem alguns exemplos como o da PECK (2018) que cita uma abordagem de seis passos para analisar os maiores riscos de segurança seguido de um leque de soluções, que podem estar no âmbito de aquisição de novos equipamentos ou mudanças administrativas. Outro exemplo é o da ICO (2019), que faz uma *checklist* geral não se preocupando apenas com segurança mas com a conformidade para cada integrante do projeto de proteção de dados ou parte do processo de regularização.

Surgiram também outros movimentos em países da América como Argentina, Chile e México. No Brasil, uma lei foi aprovada em 2018 com base na GDPR, com os mesmos princípios de restrição no tratamento de dados, direitos dos titulares e poderes do setor público. Nela também foram aprovadas medidas que tratam o dado pessoal, e multa as empresas que não entrarem em conformidade até novembro de 2020.

Este documento visa elaborar uma lista de verificação baseado na que foi produzida pela ICO, mas focando na lei brasileira.

O valor que este trabalho impulsionou a pesquisa foi contribuir na busca pela adequação dos processos à lei, visto que falta pouco tempo desde a execução deste artigo comparado à data de implementação. Ele serviu para que o corpo gestor das empresas amadurecessem em relação a lei e se adequassem à possíveis auditorias externas que pudessem ser realizadas.

2 MÉTODOS

Esta pesquisa propõe um trabalho descritivo quantitativo, enquanto visa abordar o nível de maturidade do interessado por meio de uma lista de conformidades. As perguntas abordam empresas de pequeno porte pelo nível de simplicidade das perguntas, alcançando 99% do cenário nacional, que comporta 6,4 milhões de estabelecimentos segundo o SENAI (2019).

Foi elaborado um questionário de 77 perguntas que abordam os cinco temas principais da lei Geral de Proteção de dados, com foco nos principais pontos. Para conclusão da pesquisa será utilizado como instrumento a análise dos resultados, propondo soluções iniciais para problemas que poderão surgir quando a lei entrar em vigor.

3 CONCEITOS

3.1 Lei Geral de Proteção de Dados (LGPD)

A lei 13.709/2018 – que ficou conhecida como LGPD – surgiu diante da necessidade de acompanhar o bom trabalho que já havia sendo feito na Europa com a GDPR em relação a eficácia e a aderência das empresas no quesito privacidade. A lei foi sancionada pelo ex-presidente Michel Temer em 14 de agosto de 2018 e teve início em 28 de dezembro de 2018, com período de 24 meses de tolerância para adequação dos interessados. A lei teve alguns vetos no que se refere a gestão, no entanto os conceitos foram preservados e serão apresentados a seguir.

3.1.1 Fundamentos, aplicabilidade e principais definições

A lei tem como fundamentos principais proteger os direitos fundamentais do ser humano sem atrapalhar o desenvolvimento e a globalização, com a inviolabilidade da intimidade do cidadão. Ela pode se encaixar em um dos seguintes requisitos detalhados nos Artigos 3 e 4 da LGPD para aplicação:

- Pessoa natural ou jurídica de direito público ou privado que tenha fins econômicos, que não tragam características jornalísticas, artísticas, acadêmicas, de segurança pública, de defesa nacional ou segurança do estado;
- Oferta ou fornecimento de serviços em território nacional;
- A operação de tratamento ou coleta foi realizada no Brasil;
- Não se enquadram casos de investigação e repressão de infração penal;

Para melhor entender o que será tratado nos próximos subtópicos é preciso entender alguns termos que são definidos no artigo 5, detalhados na tabela 1.

Tabela 1: Principais conceitos presentes no artigo 5

TERMO	DEFINIÇÃO
Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável
Dado sensível	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
Anonimização	Processo que desvincula o dado identificável da pessoa, tornando-o livre para tratamento.
Controlador	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; Na maioria dos casos o responsável pela empresa.
Operador	Agente que realiza o tratamento de dados pessoais em nome do controlador
Encarregado	É o cargo concedido ao DPO (*Data Protection Officer*) na GDPR, pessoa indicada pela alta gestão para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)
Tratamento	Coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, ou qualquer outra operação com dados pessoais.
Consentimento	Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
Autoridade Nacional	Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Fonte: Elaborado pelo autor(2019)

3.1.2 Requisitos para tratamento de dados pessoais

No decorrer dos artigos 10, 11, 15, 16 e 25 algumas regras foram aplicadas para dados pessoais e outras explicitamente para dados sensíveis. Na tabela 2 são detalhas as regras para dados pessoais.

Tabela 2: *Requisitos para tratamento de dado pessoal.*

Dados pessoais
• Somente dados que servem de apoio e promoção das atividades do controlador podem ser tratados;
• Para interesses do titular em relação ao negócio ou que são suas por direito com o intuito de se proteger.
• Encerrar o tratamento de dados após conclusão de finalidade do período em que esteve em tratamento, exceto quando os mesmos são anonimizados ou guardados para efeitos legais e de pesquisa;
• Os dados devem ser armazenados em formato estruturado para facilitar a portabilidade e compartilhamento.

Fonte: Elaborado pelo autor(2019)

Critérios específicos foram exigidos para dados sensíveis, que podem ser considerados um tipo especial de dado pessoal conforme descrição no subtópico anterior. Na tabela 3, estão expressos os requisitos para tratamento de dado sensível.

Tabela 3: *Requisitos para tratamento de dado sensível.*

Dados sensíveis
• O controlador deve deixar transparente o tratamento dos dados pessoais para seu legítimo interesse;
• Quando houver consentimento do usuário para aquela finalidade específica que pode a qualquer momento remover o consentimento;
• Portabilidade de dados quando solicitado pelo usuário;
• Sem consentimento do usuário, o controlador somente pode tratar o dado sensível se tiver que cumprir alguma obrigação legal, por realização de estudos, proteção da vida ou tutela da saúde; por garantia de prevenção a fraude ou segurança do titular;

Fonte: Elaborado pelo autor(2019)

3.1.3 O que vale para Controlador, Operador e Encarregado

Em relação as autoridades criadas e suas responsabilidades, os mesmos serão cobrados por meio de auditoria. Convém então conhecer as funções dos Agentes de Tratamento e do Encarregado, para em possível auditoria externa todos

estarem em conformidade. Nos subtópicos a seguir serão listadas as principais atribuições de cada um baseado nos artigos 37, 38, 41, 42, 43, 46, 47, 48 e 49.

3.1.3.1 Agentes de tratamento

Controlador e operador são os que assumem mais responsabilidades, por tratar diretamente com o tratamento de dados e serão penalizados caso não sigam com a conformidade a lei. Cada compromisso é distinto e cada um terá que se comprometer com o prejuízo pessoal causado. São elencados a seguir as principais responsabilidades:

- Manter registro das operações que realizar;
- Elaborar relatório de impacto à proteção de dados pessoais quando solicitado pela autoridade nacional;
- Reparar danos causados a violação da LGPD;
- Adotar medidas que protegem os dados de acessos não autorizados e de situações de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado, acidental ou ilícito.
- Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança;
- O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente com os seguintes atributos:
  - A descrição da natureza dos dados pessoais afetados;
  - As informações sobre os titulares envolvidos;
  - A indicação das medidas técnicas e de seguranças utilizadas para a proteção dos dados;
  - Medidas para reverter ou mitigar prejuízo;

3.1.3.2 Encarregado

Função obrigatória na empresa como citado no Artigo 41, é denominado na lei como Encarregado o responsável de comunicação entre ANPD, titular dos dados e controlador. Esta precisa ter uma autonomia do fluxo de processos para poder realizar auditorias internas de fiscalização. Tem as seguintes atividades:

- Prestar esclarecimentos sobre reclamações e tomar providências;
- Tem que ter as informações de contato explicitamente publicadas de forma clara e transparente para o titular dos dados;

3.1.4 Quais são os principais direitos dos titulares

A lei tomou parte também de esclarecer em detalhes em quais situações o usuário garante seu direito e neste tópico foi bem específica. A tabela 4 cita os principais artigos que citam algum direto do titular.

Tabela 4: Direitos do titular

Artigo	Descrição
8	Deverá existir consentimento por escrito ou outro meio que garanta a autenticidade da autorização do titular.
9	O usuário deve ter acesso facilitado as informações que estão sendo tratadas e as justificativas de tratamento.
11	Para dados pessoais sensíveis, o titular deve dar aval claro para finalidade específica do tratamento.
18	Direito de saber se está sendo tratado; o que está guardado; de atualizar o dado; de anonimização, bloqueio ou eliminação;
19	Deve utilizar os seguintes métodos para solicitar informações: simplificada ou documento formal;

Fonte: Elaborado pelo autor(2019)

3.1.5 Considerações finais sobre auditoria

Caso as cláusulas não sejam cumpridas serão atribuídas sanções administrativas previstas no o artigo 52 que, em caso de desconformidade, umas das sanções a seguir podem ser acometidas considerando fatores como a boa-fé do infrator ou reincidência:

- Advertência com prazo para adoção de medidas corretivas;
- Multa simples de até 2% (com teto de 50 milhões de reais);
- Multa diária definida pela autoridade nacional;
- Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- Eliminação dos dados pessoais a que se refere a infração;

3.3 *Checklist* para conformidade inicial

Após quase 9 meses da aplicação da lei, a realização deste artigo tem um cenário de uma economia preocupada com a não conformidade em vista da multa que poderá impactar no negócio, além dos demais prejuízos citados. Por esta razão vários autores indicam o uso de um lista de tarefas iniciais de segurança para atender o artigo 46, que explicita o uso de medidas mais atuais para proteção dos dados.

Segundo PECK (2018), todo projeto novo já deve ser pensado como *privacy by design*, que seria executá-lo tratando os dados pessoais da forma correta prevista na lei. Os processos antigos teriam que ser adaptados. A *checklist* segundo ela se dá nos seguintes passos:

1. Inventário de dados pessoais: Elencar quais são os dados e onde estão;
2. Realização de um levantamento de segurança: Fazer uma análise de como a empresa está no tocante a conformidade e o que falta para atender os controles exigidos.

3. Matriz de tratamento dos dados pessoais: quais os tipos de tratamento e para que finalidades)
4. Controle de gestão de consentimentos: Como está hoje?
5. Mapa de risco: Ordena os maiores riscos e as necessidades em um panorama.
6. Plano de ação: Investimentos necessários para a conformidade técnica, documental, procedimental e cultural.

Segundo VIVIANE, *et al.* (2018), a elaboração se baseia em um método chamado AIPD, que é um processo concebido para descrever o tratamento e avaliar a necessidade. Assim é possível gerir os riscos do tratamento dos dados pessoais avaliando-os e determinando as medidas necessárias para mitigá-los ou eliminá-los. Abaixo uma lista que descreve passos de conformidade:

1. Descrição detalhada da finalidade do tratamento;
2. Descrição detalhada das operações de tratamento;
3. Base legítima para o tratamento dos dados pessoais;
4. Avaliação da necessidade de tratamento com base na finalidade;
5. Avaliação da proporcionalidade com base na finalidade;
6. Avaliação de riscos aos direitos e liberdades do titular;
7. Medidas de mitigação de riscos e proteção dos direitos;
8. Descrição das medidas de conformação a lei de proteção de dados;

Segundo o modelo de AIPD da ICO (2019) voltado pra GDPR, baseia-se em um método de autoavaliação de impacto e foi feito para pequenas empresas ou *startups*, estas que são as mais impactadas pelas leis de proteção de dados. É um questionário em seu *website* que aborda os principais quesitos da lei europeia.

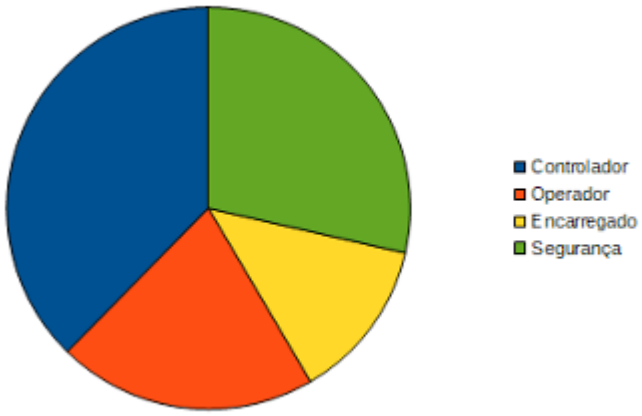
Este modelo aborda uma *checklist* para controlador, processador – semelhante ao operador na lei brasileira –, medidas de segurança, para gerenciamento e compartilhamento de dados pessoais e gerenciamento do marketing da empresa.

Neste trabalho será utilizado o método indicado por ICO (2019), por se enquadrar mais nos termos da LGPD, o que torna a inspeção mais abrangente e mais eficaz quanto ao objetivo deste artigo.

4 RESULTADOS E DISCUSSÃO

O questionário está disponível conforme publicação de RIBEIRO (2019). Os documentos possuem 77 perguntas distribuídas em cinco *checklists:* 22 perguntas de segurança, 29 perguntas para controlador, 16 perguntas para operador e 10 perguntas para Encarregado. A representação é definida no gráfico a seguir:

Figura 1: Gráfico pizza sobre Áreas da auditoria sobre a LGPD.



Fonte: Elaborado pelo autor(2019)

Na *checklist* para controlador, as perguntas foram divididas em três partes: Documentação e transparência, que abordou temas como rastreabilidade dos dados, portabilidade, consentimento, tratamento legítimo e requisição de dados por terceiros ou titular; Governança, que abordou temas como responsabilização, contratos de operador terceirizado, método *privacy by design,* padrão de boas práticas, instituição de encarregado e acompanhamento de projeto; e tratamento de incidente, que tratou o tema: respostas rápidas a incidentes.

A *checklist* para operador, funciona como uma resposta ao controlador já que este é um subordinado quase com as mesmas funções. Foi dividido em quatro partes: Relatórios ao controlador com o tema tratamento de dados pessoais; Requisições feitas pelo controlador com o tema gestão de requisições e consulta de processos; Fluxos periódicos com o tema atividades de manutenção e tratamento; e quarteirização com o tema: regras para terceirização do serviço terceiro.

Partindo para um *checklist* menor, foi criado a *checklist* para o encarregado com a subdivisão em quatro subtópicos: Relações com órgãos de fiscalização, que aborda temas como conhecimento da empresa e legislação; Relações com o titular dos dados, que aborda temas como comunicação; Relações com o encarregado, que aborda temas como gestão do tratamento; e as principais funções, que aborda temas como gerenciador de projeto e auditorias.

A *checklist* mais importante na opinião do autor RIBEIRO (2019), é a de conformidade com a segurança dos dados. A negligência deste item pode custar caro para a empresa e por isso este item foi subdivido em 4 subtópicos, dentre eles o gerenciamento de informações da empresa, que contempla toda a burocracia; a ciência da responsabilidade com o tema de conscientização; os controles de acesso que aborda temas de segurança física e digital; e os meios de proteção básicos, que contempla proteção do computador, segurança em rede, boas práticas; e backup e *restore*.

CONSIDERAÇÕES FINAIS

De acordo com os resultados obtidos, observa-se que para uma pequena ou média empresa é possível com uma simples lista de verificações poder realizar uma auditoria interna, que embasa juridicamente o viés informático de dados pessoais, tanto quanto a proteção da privacidade no meio físico. Após conhecer as principais ameaças, é possível saber onde e como agir aplicando os principais métodos de conformidade de segurança.

Visto que uma abordagem quantitativa definiu o grau de maturidade em privacidade na empresa, este estudo se completou ao contribuir com a comunidade científica e ao colaborar com a fiscalização interna das empresas.

REFERÊNCIAS

PECK, P. **PROTEÇÃO DE DADOS PESSOAIS COMENTÁRIOS A LEI N. 13.709/2018 (LGPD).** 23. ed. Saraiva jur, 2018

MALDONADO, V. *et al.* **PCOMENTÁRIOS A GDPR.** 1.ed. Thomson Reuters, 2018

WACKS. RAYMOND. **PERSONAL INFORMATION: PRIVACY AND THE LAW** . Oxford: Claredon Press, 1989. p.25

ARENHART, SÉRGIO CRUZ. **A TUTELA COLETIVA DE INTERESSES INDIVIDUAIS**. São Paulo: Revista dos Tribunais, 2013.

EQUIPE IDEAÇÃO. **COMO O BRASIL E OUTROS PAÍSES ESTÃO PROTEGENDO OS CIDADAOS**. Disponível em: <https://blogs.iadb.org/brasil/pt-br/como-o-brasil-e-outros-paises-estao-protegendo-os-dados-dos-cidadaos/>. Acesso em: 22 out. 2019.

ICO. **DATA PROTECTION SELF ASSESSMENT**. Disponível em: <https://ico.org.uk/for-organisations/data-protection-self-assessment> Acesso em: 23 out. 2019.

MARCO CIVIL. **MARCO CIVIL DA INTERNET: SEUS DIREITOS E DEVERES EM DISCUSSÃO**. Disponível em: < http://culturadigital.br/marcocivil/> Acesso em: 23 out. 2019.

PAESANI, LILIANA MINARDI. **DIREITO E INTERNET: LIBERDADE DE INFORMAÇÃO, PRIVACIDADE E RESPONSABILIDADE CIVIL**. 7. ed.. São Paulo: Atlas, 2014.

BRASIL. **DECRETO-LEI NO 13.853, DE 08 DE JULHO DE 2019. ALTERA A LEI 13.709 PARA DISPOR SOBRE A PROTEÇÃO DE DADOS PESSOAIS E PARA CRIAR A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS; E DÁ OUTRAS PROVIDÊNCIAS.** Brasília, 2018. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm>. Acesso em: 23 out. 2019.

BRASIL. **DECRETO-LEI NO 13.709, DE 14 DE AGOSTO DE 2018. LEI GERAL DE PROTEÇÃO DE DADOS**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 14 out. 2019.

BRASIL. **DECRETO-LEI NO 12.965, DE 24 DE ABRIL DE 2014. ESTABELECE PRINCÍPIOS, GARANTIAS, DIREITOS E DEVERES PARA O USO DA INTERNET NO BRASIL**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 14 out. 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. (2004A). **ABNT NBR 10.004 - RESÍDUOS SÓLIDOS: CLASSIFICAÇÃO**. Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=936>. Acesso em: 12 out. 2019.

ARCACHE, J. **THE CONTRIBUTION OF SERVICES TO MANUFACTURING COMPETITIVENESS IN BRAZIL.** Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2634434> Acesso em: 23 out. 2019.

LACNIC. **FASES DE ESGOTAMENTO IPV4**. Disponível em:<https://www.lacnic.net/1077/3/lacnic/fases-de-esgotamento-do-ipv4> Acesso em: 23 out. 2019. Acesso em: 2 out. 2019.

TECNOBLOG. **BANCO INTER DEIXA DADOS DE CLIENTES EXPOSTOS POR MAIS DE UM ANO.** Disponível em: <https://tecnoblog.net/278535/banco-inter-dados-expostos-conta-digital-pro/> Acesso em: 23 out. 2019.

JOTA. **COM GDPR, NÚMERO DE NOTIFICAÇÕES DE VAZAMENTO DE DADOS ULTRAPASSA 41 MIL CASOS.** Disponível em: <www.jota.info/pesquisa-empirica/gdpr-vazamento-de-dados-41-mil-casos-06022019> Acesso em: 23 out. 2019.

SEBRAE. **PEQUENOS NEGÓCIOS EM NÚMEROS**. Disponível em: <http://www.sebrae.com.br/sites/PortalSebrae/ufs/sp/sebraeaz/pequenos-negocios-em-numeros,12e8794363447510VgnVCM1000004c00210aRCRD> Acesso em: 23 out. 2019.

RIBEIRO. **CHECKLIST PARA LGPD.** Disponível em: <https://github.com/marcosribeiro15/LGPD>. Acesso em: 24 out. 2019