LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: IMPLEMENTAÇÃO E DETALHAMENTO DAS ATIVIDADES DA FASE 1 (*GAP ANALYSIS*) DENTRO DE UMA EMPRESA TECNOLÓGICA.

Felipe Costa Machado[1], Matheus Leandro Ferreira [2]

[1]Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC)

Resumo: A Lei Geral de Proteção de Dados (LGPD) visa regulamentar o tratamento de dados pessoais. Com o avanço da tecnologia, dia após dia, surgem novos usuários na *internet,* ocasionando um grande volume de dados trafegados. Baseando-se nisso criou-se a LGPD, no ano de 2018 com vigência em 2020, para assegurar os dados pessoais tanto por meio físico ou digital, de pessoas físicas ou jurídicas de direito público ou privado. A presente pesquisa retrata a implementação da fase 1 da Lei em uma empresa do setor tecnológico na cidade de Criciúma/SC, e ainda contempla os pontos mais importantes, destacando algumas medidas realizadas na empresa para adequação, na qual não era regulamentada em nenhuma norma da LGPD. Após compreender as normas e ter um embasamento consistente, foi possível realizar a implementação, como mapeamento de dados, desenho do ciclo de vida dos dados, aplicação da lei nas cláusulas contratuais, desenvolvimento de termos e privacidade, mapeamento de risco para identificar os setores com índices altos de riscos de vazamento de dados e realização de treinamentos para os colaboradores, tendo como maiores dificuldades a etapa de mapeamento dos dados e a reeducação dos funcionários com novas rotinas e hábitos em relação a práticas de segurança.

Palavras-chave: LGPD. Dados pessoais. Implementação. Políticas de segurança. Procedimentos.

[1] Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense (UNESC), Criciúma-SC. felipecosta@unesc.net

[2] Orientador, Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense (UNESC), Criciúma-SC. mlf@unesc.net.

ABSTRACT: *The General Data Protection Law (LGPD) aims to regulate the processing of personal data. With the advancement of technology, day after day, new users appear on the internet, causing a large volume of data. The LGPD was created in 2018, effective in 2020, to ensure personal data, both physical or digital, of individuals or legal entities and the public or private. The present research portrays the implementation of phase one in a company of the technological sector in the city of Criciúma/SC, and also contemplates the most important points, highlighting some measures carried out in the company for adequacy, in which it was not regulated in any regulation of the LGDP. After understanding the rules and having a consistent foundation, it was possible to carry out the implementation, such as data mapping, data life cycle design, law enforcement in contractual clauses, development of terms and privacy, risk mapping to identify sectors with high rates of data leakage risks and training for employees, with the greatest difficulties being the data mapping stage and the re-education of employees with new routines and habits in relation to security practices.*

Keywords: LGPD. *Personal data. Implementation. Security Policy. Procedures*.

1 INTRODUÇÃO

Atualmente é notável o aumento de usuários conectados na internet, considerando a situação pandêmica que é vivenciada. No Brasil, estudos indicam que existam 152 milhões de usuários ativos, correspondendo a 81% da população com 10 anos ou mais (CETIC, 2021).

Com base no citado acima, observa-se então, que a privacidade e a segurança digital têm se tornado um quesito de grande importância, considerando que as informações pessoais de cada usuário estão contidas nas navegações web, redes sociais e até mesmo aplicativos bancários.

Foi criada no Brasil a lei nº 13.709, em agosto de 2018, com vigência em 2020, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), que trata justamente desse assunto para promover a segurança dos dados pessoais, por meio de normas e práticas padronizadas (BRASIL, [201-?]).

A LGPD foi baseada no modelo europeu, a *General Data Protection Regulation (GDPR)*, e estabelece diretrizes sobre o tratamento de dados pessoais,

que são disponíveis tanto digitalmente como fisicamente, por pessoas físicas ou jurídicas de direito público ou privado.

O tratamento de dados estabelecido pela lei, se refere a qualquer manipulação de dados, como: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (MINISTÉRIO DA CIDADANIA, 2022).

Em 2014, houve o caso da empresa *Cambridge Analytica*, dois anos antes das eleições dos estados unidos de 2016, um aplicativo chamado *thisisyourdigitallife* coletou informações dos usuários do *Facebook*, que realizou pagamentos de uma pequena quantia a centenas de milhares de pessoas usuárias do *Facebook*, para que eles realizassem um teste de personalidade e concordassem em ter seus dados coletados para uso acadêmico. Cerca de 270 mil pessoas fizeram o teste de personalidade, sendo que se um usuário fizesse o teste, o aplicativo teria acesso a rede de amigos da rede social. Esses dados teriam sido utilizados para catalogar o perfil dos usuários e então entregar a esses perfis, materiais personalizados pró-Trump e mensagens contrárias à candidata Hillary Clinton (BBC, 2018).

No Brasil a maior parte das empresas executam tarefas em suas rotinas que acabam fazendo a coleta de dados e armazenamento dos mesmos sem o tratamento indicado. Desta forma resultando em punições e sanções, que entraram em vigor a partir do dia 1º de agosto de 2021, conforme Art 52º:

> I - Advertência, com indicação de prazo para adoção de medidas corretivas;
> II - Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III - Multa diária, observado o limite total a que se refere o inciso II;
> IV - Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - Eliminação dos dados pessoais a que se refere a infração;
> [...]
> [...]

> [...]
> [...]
> [...]
> [...]
> X - Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)
> XI - Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)
> XII - Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

Atualmente, as adequações da LGPD às pequenas e médias empresas (PME), são mais flexíveis, já que elas possuem dificuldades econômicas de investimentos e orçamentos limitados, tornando a adequação ainda mais complexa (EXAME, 2022).

Sendo assim, torna-se de suma importância esta adaptação, pois grande parte dos ataques cibernéticos, são voltados às PME, diminuindo a segurança dos dados pessoais, trazendo a incerteza sobre seu tratamento.

Cada vez mais, tem-se percebido por parte das organizações, a importância do detalhamento das atividades da etapa inicial da lei, e seu feito mostrará sobre os desafios destes processos organizacionais. Este trabalho de conclusão de curso contribui com acadêmicos da área da computação e interessados sobre a LGPD.

Este trabalho visou implantar e acompanhar adequação da fase 1 da lei geral de proteção de dados pessoais, que define a preparação, organização, desenvolvimento e implementação, governança, avaliação e melhoria, dentro de uma empresa tecnológica de Criciúma/SC, com objetivo de aumentar a aderência em relação a LGPD e diminuir referente as sanções e punições aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), utilizando o método *Gap Analysis* que segundo Lagoa (2021), com esse método é possível identificar o objetivo da empresa e sua maior deficiência em relação ao seu objetivo. Com isso, nos auxiliou a encontrar quais processos ou ferramentas podem abrir margem para possíveis sanções da LGPD.

2 TRABALHOS CORRELATOS

Para o desenvolvimento desta pesquisa foi necessário realizar um estudo sobre trabalhos referentes à LGPD, adquirindo um maior conhecimento em relação ao tema.

O artigo elaborado por Vinicius Spada Melo e Matheus Leandro Ferreira na Universidade do Extremo Sul Catarinense (UNESC), em 2022, sendo requisito para a conclusão do Curso de Ciência da Computação, relata a aplicação da Lei Geral de Proteção de Dados (LGPD) em uma empresa da região de Criciúma, focando na adequação do banco de dados à LGPD (MELO, 2022).

Além da pesquisa sobre os princípios e conceitos relacionados à LGPD, os autores destacam três categorias com os principais requisitos de segurança de dados que a lei aborda, sendo eles: avaliação, detecção e prevenção. Assim, permitindo que as empresas abordem os riscos e ameaças com diferentes perspectivas e preservem os dados de acesso não autorizados. O artigo também traz conceitos e mecanismos relacionado ao SGBD Microsoft SQL Server, no qual é utilizado pela empresa envolvida no estudo (MELO, 2022).

De acordo com o artigo, uma das maiores dificuldades encontradas ao realizar a implementação foi o levantamento dos dados pessoais, devido a quantidade de tabelas presentes no banco de dados da empresa. Ainda, após algumas reuniões foi possível elaborar algumas soluções como criar scripts que fazem o mascaramento do banco de dados antes do *backup*. Porém, os acessos ficaram sob responsabilidade do *tech lead*, fazendo com que apenas ele consiga realizar os *backups* utilizados, garantindo assim a segurança dos dados armazenados (MELO, 2022).

Por fim, como considerações o artigo traz as dificuldades encontradas em relação às mudanças de hábitos e rotinas antigas que a empresa era submetida, além da compreensão sobre os princípios que a Lei aborda. Ainda, mesmo com a burocracia envolvida, obteve-se uma maior segurança no banco de dados da empresa (MELO, 2022).

O artigo elaborado em 2021 por Vitor Elias Ferreira Carrilho na Universidade do Extremo Sul de Santa Catarina, UNESC, como requisito parcial para a conclusão do Curso em Ciência da Computação, busca compreender e implementar a LGPD em uma empresa do ramo de construção civil em Criciúma/SC (CARRILHO, 2021).

A obtenção do conhecimento sobre o tema se deu por meio de pesquisas bibliográficas e a própria Lei em questão. Assim, ao longo do trabalho foi realizada uma pesquisa sobre como a LGPD funciona e como uma empresa deve se adequar à Lei. Além disso, são relatadas informações e funções acerca dos indivíduos que têm o trabalho de gerenciar os dados pessoais, sendo eles os controladores, operadores e encarregados (CARRILHO, 2021).

Para que fosse possível a implementação da LGPD, foi necessário entender como a Lei funciona, portanto, alguns funcionários da empresa realizaram um curso e treinamento relacionado ao tema, além de outros processos burocráticos (CARRILHO, 2021).

Com isso, como conclusão, a implementação da LGPD foi realizada parcialmente dentro da empresa. Essa nova legislação é considerada extensa e complexa, no qual acaba gerando diversas dúvidas durante o processo de sua implementação. Ainda, o trabalho traz como dificuldade a mudança de hábitos e rotina da empresa e dos colaboradores. Além disso, a pesquisa ainda conta com trabalhos futuros a respeito deste tema para um conhecimento maior sobre a LGPD e sua implementação (CARRILHO, 2021).

O artigo desenvolvido em 2019 por Viviane Bezerra de Menezes Santos na Universidade Federal do Ceará, como requisito parcial para obtenção do título de Bacharela no Programa de Graduação em Direito, propõe uma análise sobre a Lei Geral de Proteção de Dados relacionada a proteção de dados e o uso do contexto do *Big Data* diante da era da privacidade virtual (SANTOS, 2019).

Durante o trabalho a metodologia utilizada foi a exploratória e qualitativa, além de pesquisas bibliográficas disponíveis e pesquisa documental. O estudo traz conceitos relacionados ao *Big Data*, no qual diz ser um termo referente a uma grande quantidade de dados, sua coleta e a interpretação deles. Além disso, a pesquisa também analisa as adaptações a serem realizadas acerca das empresas a partir da LGPD, ressaltando a importante atribuição dos programas de *compliance* visando a compatibilidade dos procedimentos internos e externos referentes à nova Legislação (SANTOS, 2019).

Ao longo da pesquisa, princípios e informações sobre o *Big Data*, *compliance* e LGPD são explicadas. A partir disso, é notável a relevância sobre questões de atenção que as empresas devem dar aos princípios da LGPD, visto que essas mudanças englobam diversos setores (SANTOS, 2019).

As considerações finais do trabalho relatam a problemática envolvendo a privacidade no meio virtual, além das considerações sobre o uso da *Big Data* pelas empresas, podendo interferir em suas questões de *compliance*, já que atualmente cresce o número de mecanismos referentes a diminuição de problemas com dados pessoais na internet, incluindo a criação da LGPD (SANTOS, 2019).

3 MATERIAIS E MÉTODOS

Esta pesquisa caracteriza-se por ser aplicada e de base tecnológica, retrata a adequação da empresa à primeira etapa da lei. Para isso, foi necessário definir o encarregado pela segurança dos dados da empresa, também conhecido como *Data Protection Officer* (DPO), bem como a cooperação do mesmo e dos colaboradores da empresa.

3.1 PASSOS PARA IMPLEMENTAÇÃO

Com base na fundamentação da lei descrita nesta pesquisa, foi possível compreender novos conceitos sobre a LGPD e todo seu sistema, servindo de auxílio para poder atingir os principais objetivos para a implementação na empresa de tecnologia.

Antes do processo de implementação foi de extrema importância conhecer a empresa e identificar os setores que realizam a coleta de dados, com isso foram analisados os fluxos e processos que fazem uso dos dados pessoais. A partir deste momento, foi realizado o mapeamento, desde a recepção dos dados até o setor de TI que faz o armazenamento dos mesmos.

Para a realização dessa etapa foi utilizado tabelas dinâmicas no *Microsoft Excel* e fluxogramas de processo, baseada na GDPR, com isso foi possível definir processos fundamentais para a segurança e implantação da lei.

Nas tabelas de mapeamento foi possível visualizar o departamento que realiza a coleta, o responsável pelo processo (nome completo), descrição do processo, agente de tratamento, atividade de tratamento, tipo de tratamento (dentro de cada atividade de tratamento), fonte (digital/analógico), ponto/forma de coleta, dados pessoais, dados sensíveis, finalidade, local de armazenamento,

compartilhamento (destinatário) e tempo de retenção, conforme mostra em parte a Figura 1.

Figura 1 – Parte da Tabela de Mapeamento

PROGRAMA DE ADEQUAÇÃO À LGPD

Processos Primários, Secundários e Gestão

MARKET

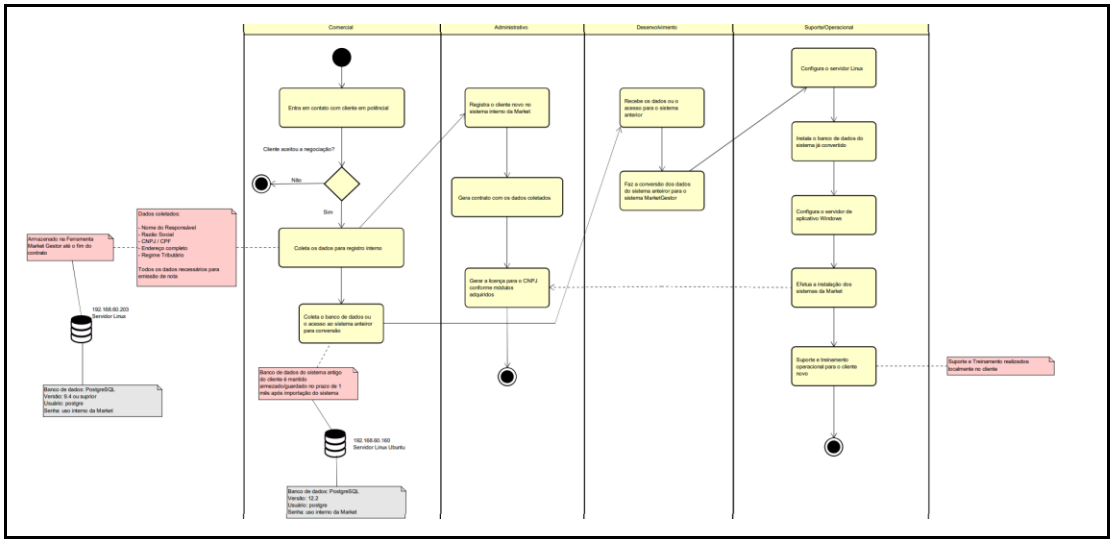
Mapeamento de Processos: Base CLIENTES

Departamento	Responsável pelo Processo (nome completo)	Descrição do Processo	Agente de Tratamento
SERVIÇOS	Tecnico de Suporte	Suporte ao usuário do sistema Market	Market - OPERADOR DE DADOS
SERVIÇOS	Tecnico de Suporte	Consulta da situação cadastral do cliente	Market - OPERADOR DE DADOS
SERVIÇOS	Desenvolvimento	Analise do erro apontado pelo cliente	Market - OPERADOR DE DADOS
SERVIÇOS	Desenvolvimento	Analise e desenvolvimento do sistema	Market - OPERADOR DE DADOS
ADMINISTRATIVO	Mxxxa Jxxxxe Pxxxxxa de Sxxxa	Cadastro do cliente	Market - CONTROLADOR DE DADOS
ADMINISTRATIVO	Mxxxa Jxxxxe Pxxxxxa de Sxxxa	Cobraça Financeira	Market - CONTROLADOR DE DADOS
ADMINISTRATIVO	Mxxxa Jxxxxe Pxxxxxa de Sxxxa	Emissão de Contrato	Market - CONTROLADOR DE DADOS
ADMINISTRATIVO	Mxxxa Jxxxxe Pxxxxxa de Sxxxa	Armazenamento de Contrato	Market - CONTROLADOR DE DADOS
COMERCIAL	Fxxxxxxxo Cxxxxs de Sxxxa	Contato comercial com o possível cliente	Market - CONTROLADOR DE DADOS
COMERCIAL	Fxxxxxxxo Cxxxxs de Sxxxa	Importação de dados	Market - CONTROLADOR DE DADOS

Fonte: Do autor.

Com a parte de mapeamento de dados pronta foi possível criar os fluxogramas para assim entender os processos e definir o ciclo de vida dos dados e como procedem para determinadas atividades, tais como implantação, suporte, assessoria e entre outras atividades realizadas pela empresa. Como mostra a Figura 2. Por exemplo, no processo de implantação em clientes, foi identificado quando a informação chegava no comercial, em qual momento passava para administração, e assim sucessivamente até completar o ciclo.

Figura 2 - Fluxograma do Mapeamento



Fonte: Do autor.

Já na etapa contratual foi necessário analisar todos os contratos junto com a equipe jurídica da empresa, assim conseguindo revisar e definir todos os itens e cláusulas dos contratos e implementar conforme a LGPD. Para adequação dos contratos elaborados para atender à LGPD, a lei exige que o consentimento do titular seja disposto em cláusulas contratuais específicas, separadas do restante do contrato.

Desta forma, nos contratos foi criada uma cláusula específica em relação aos dados pessoais chamada “O Cumprimento da Lei Geral de Proteção de Dados Pessoais pelas PARTES”, sendo composta pelos seguintes itens:

a) Considerando que haverá tratamento de dados pessoais para atender o objeto deste contrato, obrigam-se as partes a observar integralmente a legislação vigente sobre a proteção de dados pessoais, em especial a Lei 13.709/2018, respondendo cada qual, na medida de sua culpabilidade, por eventuais sanções previstas;

b) A parte que tomar conhecimento de qualquer ocorrência/incidente de segurança relacionado ao tratamento de dados pessoais objeto deste contrato, deverá comunicar imediatamente à outra Parte, para que as providências de publicação e comunicação aos titulares e à ANPD – Autoridade Nacional de Proteção de Dados sejam adotadas em conjunto, sob pena de somente uma das Partes ser responsabilizada pelo ocorrido;

c) As Partes declaram que estão em conformidade com as legislações e regulamentações brasileiras de proteção de dados pessoais e privacidade, em

especial a Lei 13.709/18. Os dados pessoais dos clientes, colaboradores e prestadores de serviço, que forem coletados e tratados pelas Partes, serão utilizados para o exercício da prestação de serviços desta;

d) As Partes ainda asseguram que seus empregados ou os prestadores de serviços que venham a ter acesso aos Dados Pessoais no contexto deste CONTRATO, deverão cumprir com as disposições legais aplicáveis em matéria de proteção de dados pessoais, não cedendo ou divulgando tais dados pessoais a terceiros, nem deles fazendo uso para quaisquer fins exceto para a finalidade deste CONTRATO;

e) Novas versões e funcionalidades do software eventualmente disponibilizadas aos usuários, que possam intervir no tratamento dos dados pessoais, serão concebidas em conformidade com a LGPD;

f) Quando estiver cumprindo a função de operadora dos dados pessoais de seus clientes e parceiros, a CONTRATADA fará a gestão das ferramentas utilizadas para o tratamento dos mesmos, promovendo testes periódicos para identificação e imediata correção de eventuais vulnerabilidades que venham a ser identificadas, em atendimento ao art. 39 da LGPD;

g) Os dados pessoais dos titulares tratados neste CONTRATO, deverão ser deletados pelas PARTES, imediatamente após o término da vigência do contrato firmado quando a finalidade e temporalidade de guarda forem alcançadas, conforme previsto nos artigos 15 e 16 da LGPD.

Observando os tópicos esclarecidos anteriormente, concluiu-se com a equipe jurídica que em relação ao tratamento de dados na parte de contratos, está objetiva e clara de como os dados foram tratados e em conformidade com a lei, deixando os clientes da empresa consciente quando se trata de seus dados pessoais.

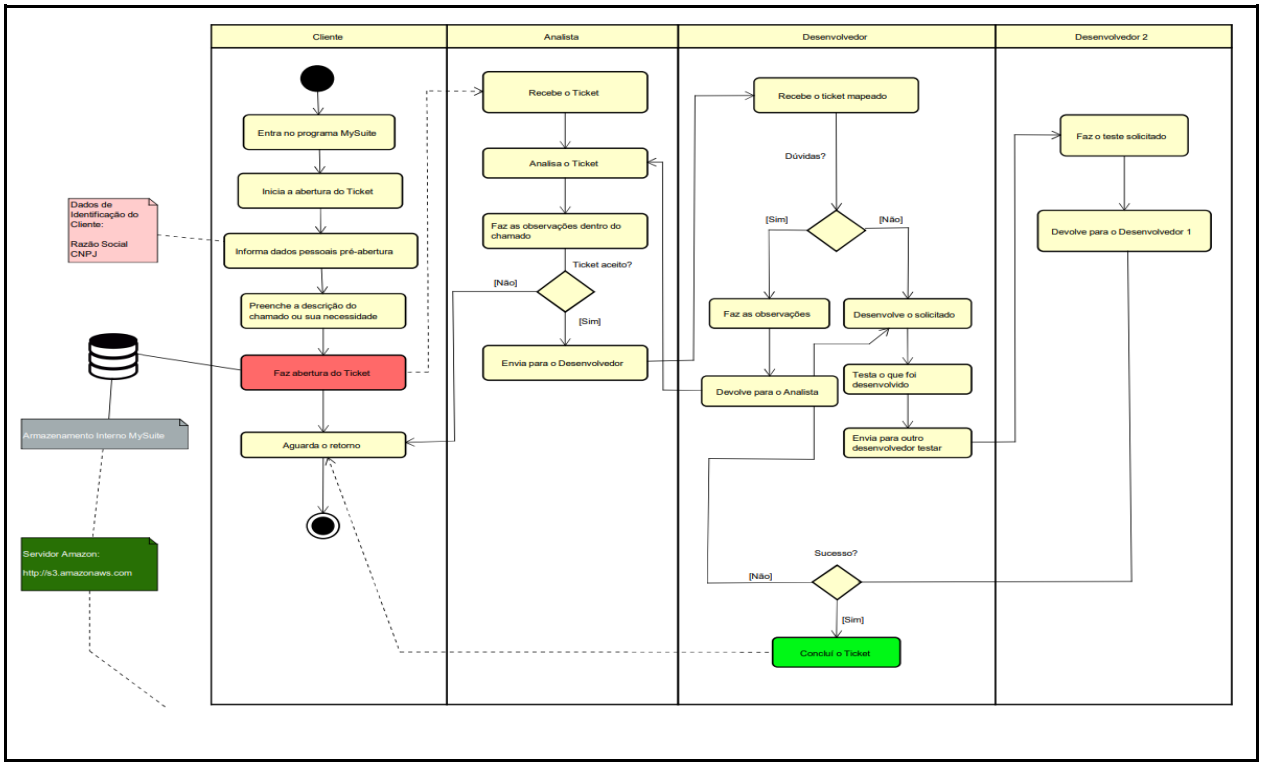
Outra tarefa foi adequação do site da empresa em relação da LGPD, onde observou-se a necessidade de criar os termos de políticas de privacidade, novamente com a equipe jurídica, sendo que nada mais seria do que o contrato entre o usuário do site e o proprietário da página, possibilitando acesso os direitos de deveres de forma facilitada. Após o site estar de acordo com as demandas impostas pela LGPD, para maior segurança, trocou-se o site de servidor, pois o mesmo ficava em servidores da empresa. O mesmo, que apesar de toda a infraestrutura de TI ter passado por uma revisão, sobre *firewall's*, antivírus, manutenções preventivas, assim mantendo a

segurança na rede de computadores, a integridade da segurança dos dados foi priorizada. Com isso, foi contratada a empresa *locaweb* que realiza a hospedagem de sites, para hospedar o site da empresa, assim assegurando que todos os dados estariam em nuvem e garantindo a integridade das informações pela contratada.

Para a realização de atendimentos ao cliente, foi utilizada a ferramenta *mySuite,* que possibilita ao cliente, realizar a abertura de *ticket* para receber um atendimento. Nessa etapa também foi realizado o mapeamento dos dados, identificando como essas informações chegam ao setor de atendimento, assim podendo definir se há algum tipo acesso aos dados do cliente.

Nessa etapa não foi possível fazer restrições no acesso às informações do cliente, mas com objetivo de transparência com o mesmo, foi configurada uma mensagem de ciência ao cliente na criação de *ticket,* assim conseguiu-se de forma simples e clara explicitar como os dados seriam tratados.

Figura 3: Fluxograma e análise da ferramenta *mySuite*



Fonte: Do autor.

Umas das etapas mais importantes e após o mapeamento de dados, é a análise de riscos, na qual foi realizada em todos os setores, buscando identificar qual o grau de risco de vazamentos de dados. Para essa etapa também foi utilizado a ferramenta *Microsoft Excel*, sendo possível mapear as atividades, descrição do

mesmo, descrição do risco, tratamento, classificação do grau, responsável, prazo, e por último o custo da medida, conforme ilustra a Figura 4. Nesta etapa foi utilizado o método da *Gap Analisys* para assim identificar onde possivelmente seria o maior risco de vazamentos de dados, conseguiu-se assim, iniciar o tratamento de dados e realizar treinamentos aos colaboradores desse setor. Com isso foi possível cada vez mais diminuir a aderência da empresa em relação às sanções e penalidades aplicadas pela lei.

Figura 4: Mapeamento de riscos

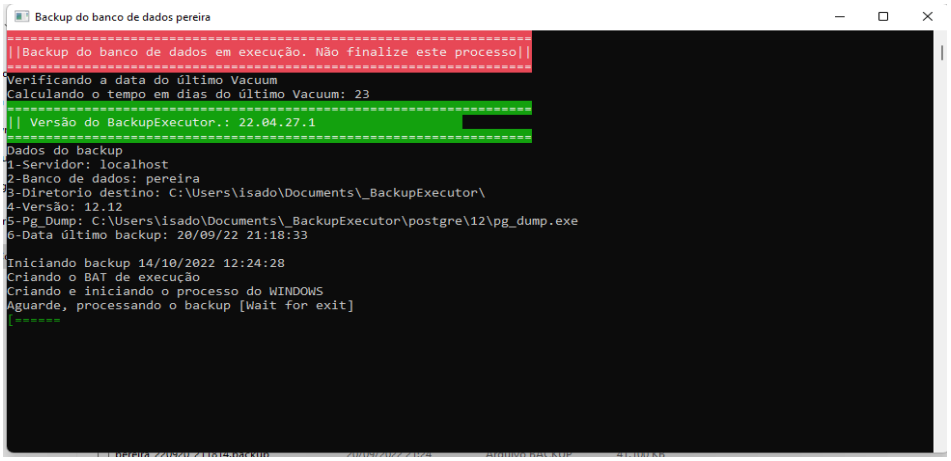
MAPEAMENTO DE RISCO

	ATIVIDADE PRINCIPAL	DESCRIÇÕES DO RISCO	TRATAMENTO	CLASSIFICAÇÃO	RESPONSÁVEL	PRAZO	CUSTO DA MEDIDA
R-001	Homologação de Boletos	Envio do arquivo com informações pessoais via e-mail para o banco	Vazamento da informação por parte do desenvolvedor	EVITAR	ALTO	Rxxxxl Sxxxr de Oxxxxxxa	N/A	R$ -
			Envio para e-mail incorreto	EVITAR	ALTO	Rxxxxl Sxxxr de Oxxxxxxa	N/A	R$ -
			E-mail pode ser interceptado	EVITAR	ALTO	Rxxxxl Sxxxr de Oxxxxxxa	N/A	R$ -
			Arquivo aberto e sem criptografia ou senha	MITIGAR	MÉDIO	Rxxxxl Sxxxr de Oxxxxxxa	N/A	R$ -
			Sistema operacional da maquina desenvolvedor desatualizada	EVITAR	MÉDIO	Rxxxxl Sxxxr de Oxxxxxxa	N/A	R$ -
			Maquina do desenvolvedor sem anti-virus	EVITAR	MÉDIO	Rxxxxl Sxxxr de Oxxxxxxa	N/A	R$ -
			Desenvolvedor não apaga o e-mail contendo o arquivo após homologado	EVITAR	MUITO BAIXO	Rxxxxl Sxxxr de Oxxxxxxa	N/A	R$ -
		Obtenção da base de dados do sistema anterior	Vazamento do banco e sua respectiva senha pelo suporte responsável	EVITAR	ALTO	Rxxxxl Exxxxxxg	N/A	R$ -
			Vazamento do banco e sua respectiva senha pelo desenvolvedor responsável	EVITAR	ALTO	Rxxxxl Exxxxxxg	N/A	R$ -
			Armazenamento do banco no pen-drive pessoal do suporte responsável	EVITAR	ALTO	Rxxxxl Exxxxxxg	N/A	R$ -
			Envio do banco de dados via FTP	MITIGAR	MÉDIO	Rxxxxl Exxxxxxg	N/A	R$ -
			Sessão do FTP deixada aberta na maquina do cliente	EVITAR	ALTO	Rxxxxl Exxxxxxg	N/A	R$ -
			Envio do banco de dados zipado ao google drive pessoal	EVITAR	ALTO	Rxxxxl Exxxxxxg	N/A	R$ -
			Maquina do cliente sem firewall e/ou antivirus	ACEITAR	MUITO BAIXO	N/A	N/A	R$ -
R-002	IMPORTAÇÃO DO SISTEMA	Obtenção da base de dados do sistema anterior	Vazamento do banco pelo suporte responsável	EVITAR	ALTO	Rxxxxl Exxxxxxg	N/A	R$ -
			Vazamento do banco pelo desenvolvedor responsável	EVITAR	ALTO	Hxxxxn Pxxxxi	N/A	R$ -
			Armazenamento do banco no pen-drive pessoal do suporte responsável	EVITAR	ALTO	Rxxxxl Exxxxxxg	N/A	R$ -
			Envio do banco de dados via FTP	MITIGAR	MÉDIO	Rxxxxl Exxxxxxg	N/A	R$ -
			Sessão do FTP deixada aberta na maquina do cliente	EVITAR	ALTO	Rxxxxl Exxxxxxg	N/A	R$ -
			Envio do banco de dados zipado ao google drive pessoal	EVITAR	ALTO	Rxxxxl Exxxxxxg	N/A	R$ -
			Maquina do cliente sem firewall e/ou antivirus	ACEITAR	MUITO BAIXO	N/A	N/A	R$ -
		Exportação do banco de dados já finalizado	Maquina do desenvolvedor sem antivirus e/ou firewall ativado	EVITAR	MÉDIO	Hxxxxn Pxxxxi	N/A	R$ -
			Vazamento durante o processo de exportação	EVITAR	ALTO	Hxxxxn Pxxxxi	N/A	R$ -
			Copia da exportação em local pessoal do desenvolvedor	EVITAR	ALTO	Hxxxxn Pxxxxi	N/A	R$ -
			Vazamento de informações pessoais por parte do desenvolvedor	EVITAR	ALTO	Hxxxxn Pxxxxi	N/A	R$ -
			Desenvolvedor manter o banco exportado em sua maquina após a importação do cliente	MITIGAR	MÉDIO	Hxxxxn Pxxxxi	N/A	R$ -

Fonte: Do autor.

Como foi realizada a análise de risco, assim foi observado e classificado junto com o DPO, que umas das falhas que poderia ser de alto risco e que não era possível ter o controle da empresa, seria o banco de dados do cliente que fica nos servidores do contratante. Com isso em uma reunião com o DPO, foi decidido desenvolver um *script* que realiza o *backup* nos servidores locais de cada cliente, e criptografa o banco de dados, conforme mostra a Figura 5, evitando assim que em casos de ataques, o invasor consiga ter acesso a esses dados, ilustrada na Figura 7. A criptografia utilizada foi a *Advanced Encryption Standard* (AES) por ser umas das mais seguras, sendo uma cifra de bloco simétrico com a qual se pode criptografar e decriptografar dados. Esse algoritmo tem a capacidade de usar chaves criptográficas de 128, 192, 256 bits para realizar esses processos de cifragem.

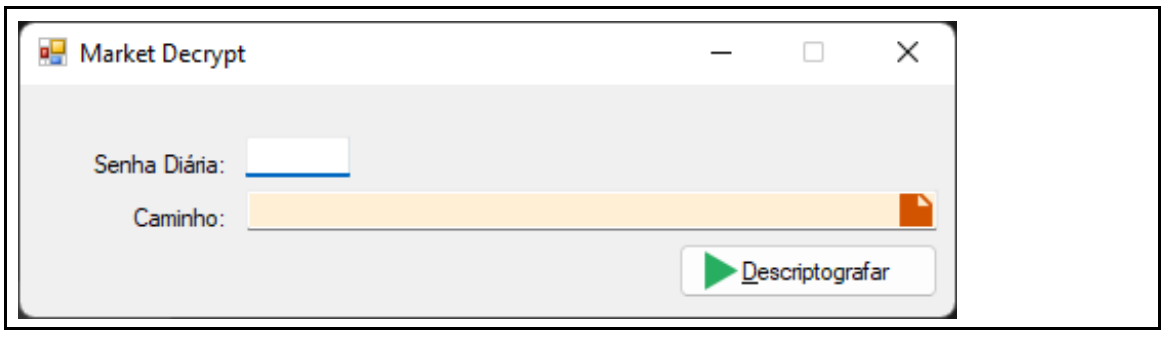
Figura 5: *Script* de *Backup*



Fonte: Do autor.

Outra ferramenta que foi desenvolvida foi a de decriptografar o banco de dados, para que caso o suporte tivesse a necessidade de realizar algum processo na base de dados, o suporte conseguisse decriptografar. Esse *script* possui uma senha diária na qual somente o suporte e o desenvolvedor, conseguem gerar essa senha localmente na empresa, aumentando a segurança e diminuindo o risco de vazamentos desses dados. As duas ferramentas citadas acima foram desenvolvidas na linguagem de programação *C Sharp,* e foi escolhida por que conforme Bill Wagner (2022), é possível desenvolver *scripts* mais seguros, devido a sua tipagem ser forte e orientada a objetos, conforme (Figura 6).

Figura 6: *Software* de Descriptografar



Fonte: Do autor.

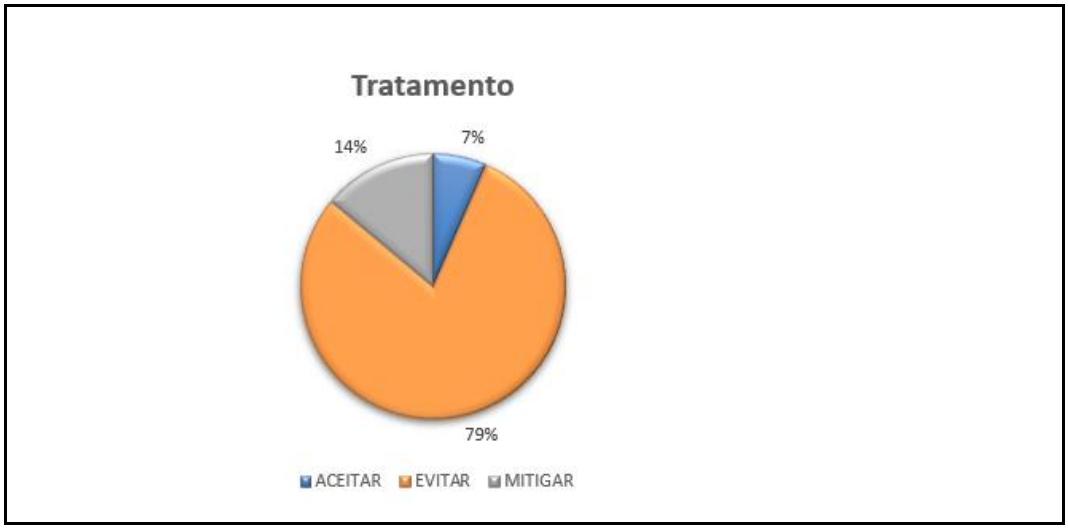
Figura 7: Ao realizar *restore* da base criptografada

Fonte: Do autor.

Em relação aos colaboradores, foi realizada a apresentação de resultados da implementação e treinamentos em relação a LGPD, foi também realizado um *workshop*, onde foi possível reunir todos os colaboradores da empresa, torná-los aptos a fazer o tratamento de dados pessoais e ficarem cientes de qual a situação da empresa em relação aderência a LGPD.

Nesta pesquisa foi possível realizar análises, uma delas aplicada no mapeamento de riscos, na qual foi observado onde estavam os riscos e quais seus níveis. Com isso defini-se qual seria o tratamento do risco, como mitigar, evitar ou aceitar. Com esses dados, foi então definido em qual grau a empresa estava sobre as sanções e punições da lei apenas realizando a primeira fase da implementação, conforme mostra a Figura 8.

Figura 8: Gráfico Mapeamento de Risco



Fonte: Do autor.

4 RESULTADOS E DISCUSSÃO

Este trabalho foi desenvolvido com base na aplicação da fase 1 da LGPD, em uma empresa do setor tecnológico da região de Criciúma/SC. A maior dificuldade encontrada durante a implementação, foi realizar o mapeamento de dados. A empresa possui diversos setores que transitam dados pessoais, e mapeá-los nos custou alguns dias. A dificuldade nesta etapa também foi identificada no artigo de Carrilho (2021), que realizou a implementação em uma empresa de engenharia.

Uma das etapas mais importantes em relação a implementação da LGPD, foi a definição do DPO. O responsável passou por uma capacitação pela equipe jurídica obtendo conhecimento adequado sobre a lei para assim, garantir os dados da empresa.

Uma deficiência que foi possível identificar através de uma reunião com o DPO, foi sobre os bancos de dados dos clientes, que constantemente solicitam suporte. Em determinados momentos há necessidade de uma análise detalhada, onde o programador necessita ter o banco de dados do cliente importado dentro da empresa. A responsabilidade de manter o *backup* do banco de dados é do cliente, porém nem sempre é seguro. O gerador de backup também é totalmente sem criptografia, fazendo os dados ficarem vulneráveis a ataques cibernéticos.

Após diversas reuniões com o DPO, chegou-se a conclusão de desenvolver um *script* que realizasse o *backup* do cliente criptografado, com um tipo de criptografia

que fosse segura e difícil de ser quebrada. Desta forma foi desenvolvido uma ferramenta em C *Sharp*, para realizar o backup do banco de dados no próprio cliente, e quando fosse encaminhado para os servidores, já estivesse criptografado, sem nenhuma interferência no intervalo entre o cliente e servidor, evitando algum tipo de ataque ou vazamentos de dados.

Além disso, o suporte ou desenvolvedor, em determinados momentos, precisam ter acesso ao banco de dados do cliente para realizar testes, manutenção e análises. Por isso foi desenvolvida também uma ferramenta para descriptografar o arquivo. Para realizar este processo, o *software* necessitava de uma chave diária, na qual somente o desenvolvedor e suporte conseguiam liberar para descriptografar.

Entre as diversas tarefas que foram realizadas, uma delas foi adequação do site conforme a lei, assim incluindo aviso de privacidade, solicitação de privacidade, aviso de *cookies* e os termos de uso, com isso foi possível deixar claro para o titular como será o tratamento dos seus dados ao utilizar o site.

Em relação a parte contratual, foi outra etapa que custou vários dias e diversas reuniões com a equipe jurídica, considerando que LGPD é nova, até definir as cláusulas necessárias para deixar os contratos de acordo com a lei, apesar de levar um certo tempo, não houve muita dificuldade, sendo que a equipe jurídica tinha certo conhecimento na área.

Uma das últimas etapas e não menos importante, foi sobre os treinamentos dos colaboradores, para assim ter ciência de como a empresa estava em relação a lei, e como devem se comportar e executar em relação aos tratamentos de dados pessoais, realizar boas práticas e novas rotinas.

5 CONCLUSÃO

Na presente pesquisa foi acompanhada a implementação parcial da LGPD em uma empresa de tecnologia da região de Criciúma/SC. Como a Lei Geral de Proteção de Dados é nova, surgiram algumas dúvidas, nas quais foram sanadas com o desenvolvimento do trabalho.

Com a complexidade da lei, demandou estudos e reuniões com a equipe jurídica mesmo durante a implementação, assim foi possível sanar as dúvidas que foram levantadas durante o processo, possibilitando a compreensão mais profunda das normas da lei. Após as dificuldades e compreensão da lei, foram apontados os

dados que são considerados dados pessoais (RG, CPF, gênero, data de nascimento, local de nascimento, telefone, endereço residencial) e dados sensíveis (origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas etc.).

Apesar do curto período para implementação da LGPD, foi possível finalizar a implementação da fase 1 da LGPD, a metodologia da *Gap Analisys* se provou ser eficiente, pois foi possível identificar qual era o estado atual da empresa e quais seus objetivos, assim definindo onde estava a maior deficiência e iniciar a implementação. Por meio do gráfico ilustrado na Figura 8, foi possível comprovar que com a elaboração do mapeamento de risco, possibilitou ter uma visão melhor em relação a situação da empresa até a conclusão deste trabalho.

Um dos pontos mais difíceis de implementar foi a mudança dos hábitos e rotinas dos funcionários, acostumando-os com boas práticas, como bloquear a tela dos seus computadores ao deixá-los, não compartilhar arquivos relacionados a empresa, como fotos, documentos, dados de clientes e de funcionários com amigos ou nas redes sociais.

Para trabalhos futuros recomenda-se a busca por referencial teórico sobre a segunda fase da implementação da LGPD e sua aplicação, como também cartilhas e treinamentos para novos funcionários, para que ainda possa evitar mais sanções aplicadas pela ANPD. Além disso, há conteúdos sobre GDPR que podem ser explorados.

REFERÊNCIAS

ACSP. LGPD: como adequar o site da sua empresa à legislação?. como adequar o site da sua empresa à legislação?. Disponível em: https://acsp.com.br/publicacao/s/lgpd-como-adequar-o-site-da-sua-empresa-a-legislacao. Acesso em: 16 jun. 2022.

AES **–** Padrão de criptografia avançado: o que é e como funciona. 2021. Disponível em: https://cryptoid.com.br/criptografia/aes-padrao-de-criptografia-avancado-o-que-e-e-como-funciona/. Acesso em: 07 out. 2022.

ALIX (org.). Diagnóstico de Maturidade da LGPD. 2021. Disponível em: https://www.alix.com.br/post/diagn%C3%B3stico-de-maturidade-da-lgpd#:~:text=O%20diagn%C3%B3stico%20de%20maturidade%2C%20as,requisitos%20e%20exig%C3%AAncias%20da%20Lei.. Acesso em: 16 jun. 2022.

ARTESE, Gustavo; IÓRIO, Pedro. ANPD e as sanções da LGPD:: o que, quando, quem e como. o que, quando, quem e como. 2021. Disponível em: https://tiinside.com.br/03/08/2021/anpd-e-as-sancoes-da-lgpd-o-que-quando-quem-e-como/. Acesso em: 08 jun. 2022.

BBC NEWS (ed.). Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em: 28 fev. 2022.

BILL WAGNER (ed.). Escrever um código C# seguro e eficiente. Disponível em: https://learn.microsoft.com/pt-br/dotnet/csharp/write-safe-efficient-code. Acesso em: 29 nov. 2022.

BOFF, Salete Oro; FORTES, Vinícius Borges. A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil. Sequência (Florianópolis), n. 68, p. 109-127, 2014.

BRANDAO, Graziela. O que é o mapeamento de dados? Disponível em: https://blconsultoriadigital.com.br/mapeamento-de-dados/. Acesso em: 12 jun. 2022.

BRASIL. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. (org.). Perguntas Frequentes – ANPD. 2021. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd#c1. Acesso em: 16 maio 2022.

BRASIL. Governo Federal. Ministério da Cidadania. Lei Geral de Proteção de Dados Pessoais (LGPD). [201-?]. Disponível em: https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd. Acesso em: 28 fev. 2022.

BRASIL. SERPRO. (org.). DADOS ANONIMIZADOS: o que são dados anonimizados, segundo a lgpd. O que são dados anonimizados, segundo a LGPD.

[201-?]. Disponível em: https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-anonimizados-lgpd. Acesso em: 16 maio 2022.

BRASIL. SERPRO. (org.). DADOS PESSOAIS: o que são dados pessoais, segundo a lgpd. O que são dados pessoais, segundo a LGPD. [201-?]. Disponível em: https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-pessoais-lgpd. Acesso em: 16 maio 2022.
BRASIL. SERPRO. (org.). DADOS SENSÍVEIS: o que são dados sensíveis, de acordo com a lgpd. O que são dados sensíveis, de acordo com a LGPD. [201-?]. Disponível em: https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-sensiveis-lgpd. Acesso em: 16 maio 2022.

BRASIL. SERPRO. (org.). O QUE MUDA COM A LGPD: o que é a lei geral de proteção de dados pessoais? dê um "giro" pela lei e conheça desde já as principais transformações que ela traz para o país. O que é a Lei Geral de Proteção de Dados Pessoais? Dê um "giro" pela lei e conheça desde já as principais transformações que ela traz para o país. [201-?]. Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd. Acesso em: 16 maio 2022.

CARRILHO, Vitor Elias Ferreira. IMPLEMENTAÇÃO DA LGPD EM UMA EMPRESA DO RAMO DE CONSTRUÇÃO CIVIL EM CRICIÚMA/SC. 2021. 20 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense (Unesc), Criciúma, 2021.

CETIC (org.). Cresce o uso de Internet durante a pandemia e número de usuários no Brasil chega a 152 milhões, é o que aponta pesquisa do Cetic.br. 2021. Disponível em: https://cetic.br/pt/noticia/cresce-o-uso-de-internet-durante-a-pandemia-e-numero-de-usuarios-no-brasil-chega-a-152-milhoes-e-o-que-aponta-pesquisa-do-cetic-br/. Acesso em: 22 fev. 2022.

CORTAZIO, Renan Soares. Bancos de dados no Brasil: uma análise do sistema credit scoring à luz da LEI N. 13.709/2018 (LGPD). REVISTA ELETRÔNICA DA PGE-RJ, v. 2, n. 3, 2019.

CRAVO, Victor et al (org.). GUIA DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 16 maio 2022.

DE ALMEIDA, Ana Carolina Brito et al. LGPD em Ambientes de Bancos de Dados nas Organizações. Sociedade Brasileira de Computação, 2019.

DIGITAL, Direito (ed.). Quais as atribuições do encarregado (DPO) segundo a Lei de Proteção de Dados. [2020?]. Disponível em: https://assisemendes.com.br/funcoes-dpo/. Acesso em: 11 jun. 2022.

DONDA, Daniel. Guia Prático de Implementação da LGPD. São Paulo: Labrador, 2020. 144 p.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico Journal of Law [EJJL], v. 12, n. 2, p. 91-108, 2011.

EXAME. LGPD: uma nova resolução flexibiliza obrigações para as PMEs. 2022. Disponível em: https://exame.com/pme/lgpd-uma-nova-resolucao-flexibiliza-obrigacoes-para-as-pmes/. Acesso em: 09 mar. 2022.

FARIA, Andrea Filomeno; POLI, Tatiana Brenand Bauer. Adequação de contratos à LGPD: necessidade das empresas a partir de 2021. necessidade das empresas a partir de 2021. 2021. Disponível em: https://www.conjur.com.br/2021-dez-11/direito-digital-adequacao-contratos-lgpd-necessidade. Acesso em: 08 jun. 2022.

FREITAS, Carla. Sendo assim, caso os itens acima não se apliquem, orienta-se deixar claro as situações, informando que os dados serão tratatos pela organização não havendo o compartilhamento com pessoas fisicas ou juridicas do meio externo. 2019. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2019/elabora-politica-privacidade-aderente-lgpd-dados-pessoais#:~:text=A%20pol%C3%ADtica%20de%20privacidade%20%C3%A9,de%20Dados%20Pessoais%20(LGPD).. Acesso em: 12 jun. 2022.

GARCIA, Lara Rocha; FERNANDES, Edson Aguilera; GONÇALVES, Rafael Augusto Moreno; BARRETTO, Marcos Ribeiro Pereira. Lei Geral de Proteção de Dados Pessoais (LGPD): guia de implantação. São Paulo: Blucher, 2020. 128 p.

GOIÁS, Ead Puc (org.). O que é workshop, para que serve e como planejar o evento? 2020. Disponível em: https://ead.pucgoias.edu.br/blog/workshop-planejar-evento. Acesso em: 16 jun. 2022.

LAGOA, Marco. GAP Analysis: o que é e como esse processo ajuda sua ti. o que é e como esse processo ajuda sua TI. 2021. Disponível em: https://witec.com.br/gap-analysis/. Acesso em: 29 nov. 2022.

LIMA, Ana Paula Moraes Canto de; ALMEIDA, Dionice de; MAROSO, Eduardo Pereira. LGPD: lei geral de proteção de dados: sua empresa está pronta?. São Paulo: Literare Books International., 2020. 188 p.

MARCONDES, José Sérgio. Política de Segurança:: o que é, qual sua importância, como criar. O que é, Qual sua Importância, Como criar. 2022. Disponível em: https://gestaodesegurancaprivada.com.br/politica-de-seguranca-o-que-e-qual-sua-importancia-como-criar/. Acesso em: 16 jun. 2022.

MELO, Vinicius Spada. APLICAÇÃO DA LGPD EM UMA EMPRESA DA REGIÃO DE CRICIÚMA:: estudo de caso em banco de dados. 2022. 24 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade do Extremo Sul Catarinense, Criciúma, 2022.

O IMPACTO da segurança frágil das PMEs. 2022. Disponível em: https://www.aim7.com.br/conteudo/artigos/o-impacto-da-seguranca-fragil-das-pmes/. Acesso em: 09 mar. 2022.

POHLMANN, Sérgio Antônio. LGPD Ninja: entendendo e implementando a lei geral de proteção de dados nas empresas. Nova Friburgo: Editora Fross, 2019.
REGULATION, General Data Protection. General data protection regulation (GDPR). Intersoft Consulting, Accessed in October 24, v. 1, 2018.

SABINO, Richard. GESTÃO DA SEGURANÇA DA INFORMAÇÃO ORIENTADO A LGPD: IMPACTOS DA IMPLANTAÇÃO DAS NORMAS LGPD NOS PROCESSOS DA ADM SISTEMAS LTDA. 2020. 21 f. TCC (Graduação) - Curso de Tecnólogo em Gestão da Tecnologia da Informação, Universidade do Sul de Santa Catarina, Palhoça, 2020.

SANTOS, Viviane Bezerra de Menezes. Lei Geral de Proteção de Dados: Fundamentos e Compliance. 2019. 54 f. Monografia (Graduação em Direito) - Faculdade de Direito, Universidade Federal do Ceará, Fortaleza, 2019

SERVICE (org.). A importância da avaliação de riscos no processo de adequação à LGPD. 2020. Disponível em: https://service.com.br/a-importancia-da-avaliacao-de-riscos-no-processo-de-adequacao-a-lgpd/#:~:text=Como%20a%20avalia%C3%A7%C3%A3o%20de%20risco,e%20a%20gravidade%20dos%20riscos%E2%80%9D.. Acesso em: 16 jun. 2022.

REINO UNIDO. INFORMATION COMMISSIONER'S OFFICE. (ed.). Documentação. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/. Acesso em: 10 ago. 2022.

TECH, PRIVACY. Empresas adequadas à LGPD ainda são minoria, segundo RD Station. 2021. Disponível em: https://www.privacytech.com.br/lgpd/empresas-adequadas-a-lgpd-ainda-sao-minoria-segundo-rd-station,402553.jhtml. Acesso em: 19 mar. 2022.

WEBER, Demétrio. Como se adaptar à Lei Geral de Dados. 2020. Disponível em: https://www.educa2022.com/post/como-se-adaptar-%C3%A0-lei-geral-de-prote%C3%A7%C3%A3o-de-dados. Acesso em: 16 jun. 2022.