

IMPLEMENTAÇÃO DA LGPD EM UMA EMPRESA DO RAMO DE CONSTRUÇÃO CIVIL EM CRICIÚMA/SC

Vitor Elias Ferreira Carrilho¹, Prof. Dr. Rogério Antônio Casagrande¹

¹Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC) –
Criciúma – SC – Brasil

vecarrilho@hotmail.com, roc@unesc.net

RESUMO: A Lei Geral de Proteção de Dados (LGPD) tem como objetivo regulamentar o tratamento de dados pessoais no âmbito do País. O presente trabalho tem o objetivo de apresentar a implementação da LGPD em uma empresa do ramo de construção civil em Criciúma/SC. Foram estabelecidas, entre outras, medidas e políticas de segurança para os processos internos, boas práticas aos colaboradores, a coleta de assinaturas dos funcionários para permitir o uso de sua imagem e dados, criado relatórios de incidente para mapear os setores com maiores índices de impacto no caso de algum tipo de vazamento de dados. Utilizando a bibliografia disponível e a própria lei em questão, este trabalho contextualiza brevemente a lei em questão, citando seus pontos mais importantes, e um conjunto de procedimentos que possibilitou a implementação parcial da LGPD no âmbito da empresa. Após um curto período de tempo para implementação da LGPD na empresa, a mesma apresentou dificuldades como alto número de documentos gerados, dúvidas referente a lei dentro da empresa e reeducar colaboradores com novas práticas de segurança.

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

ABSTRACT: *The General Data Protection Regulation from Brazil (LGPD) has the objective to regulate the treatment of personal data within the country. This research aims to present the implementation of the LGPD in a construction company in Criciúma/SC. It established, among others, security measures and policies for internal processes, good practices for employees, the collection of employee signatures to allow the use of their image and data, and created incident reports to map the sectors with the highest impact rates in case of some kind of data leak. Using articles and the law itself, this paper briefly contextualizes the law in question, citing its most important points, and a set of procedures that enabled the partial implementation of LGPD within the company. After a short period of time to implement the LGPD in the company, it presented difficulties such as the high number of documents generated, doubts regarding the law within the company and re-educating employees with new security practices.*

Keywords: LGPD. Personal data. Implementation. Security policy. Procedures

1 INTRODUÇÃO

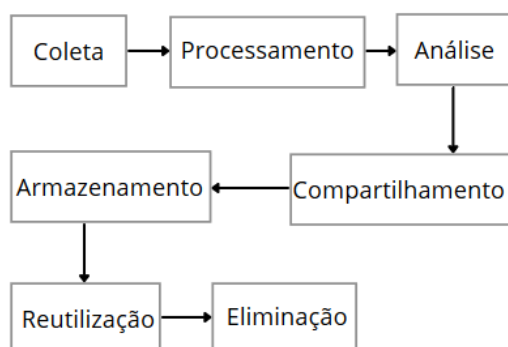
A questão da privacidade e segurança digital é um assunto que vem ganhando importância nos dias atuais, devido à facilidade de acesso à internet e inúmeras informações pessoais contidas na mesma.

Em 23 de abril de 2014 foi sancionada no Brasil a lei nº 12.965, mais conhecida como “Marco Civil da Internet”, que segundo seu Art 1º, garante direitos e deveres para aqueles que utilizarem a internet no território nacional, sendo está a primeira lei de privacidade digital no Brasil.

Devido ao grande aumento de usuários na internet, só no Brasil em 2019 82,7% das casas tinham acesso à internet (IBGE, 2019), e a utilização oculta de seus dados pessoais, possivelmente danosa ao titular, se faz necessária uma nova lei regulamentadora que proteja os dados de pessoas físicas.

Em 14 de agosto de 2018 é sancionada no Brasil a lei nº 13.709, mais conhecida como Lei Geral de Proteção de Dados (LGPD), que segundo seu Art 1º tem como objetivo proteger os dados pessoais quando tratados por empresas ou pessoas fictícias (Figura 1), garantindo assim liberdade e privacidade ao titular, que para Fernandes et al. (2020), é definida como o direito de ser deixado só, sem a interferência do Estado na vida do indivíduo.

Figura 1 – Ciclo de Vida dos Dados Pessoais



Esta lei tem como base a *General Data Protection Regulation* (GDPR), lei regulamentadora de proteção de dados na União Europeia nº 2016/679. Em 2016 foi definido que as empresas na União Europeia teriam no total dois anos para adaptarem suas rotinas de coleta, armazenamento e exclusão de informações pessoais conforme a GDPR, que visa proteger a privacidade e liberdade das

pessoas físicas, dando a elas o direito sobre seus dados (CÉSAR; ASPIS; CHAVES, 2019).

Atualmente no Brasil grande parte das empresas, devido suas rotinas, sistemas internos e externos, acabam realizando o tratamento de algum tipo de dado de pessoa física sem a proteção adequada no mesmo, algo que poderá acarretar em sanções administrativas a partir do dia 1º de agosto de 2021, conforme Art 52º da lei nº 13.709/2018.

Os tipos de informações pessoais podem ser separados em dado pessoal que é definido no Art 5º inciso I da lei federal nº 13.709/2018 como uma informação utilizada para identificar uma pessoa natural, ou dado sensível, trazido pelo Art 5º inciso II da lei nº 13.709/2018, podendo ser uma informação relacionada à sua “[...] 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” (Brasil, 2018).

Para executar o tratamento dos dados é necessário estar de acordo com pelo menos uma de um conjunto de diretrizes, conhecidas como base legal, que segundo Ramos (2019, p. 11) é uma autorização prevista pela LGPD para que o tratamento seja realizado.

As diretrizes são:

- I) Mediante o fornecimento de consentimento pelo titular;
- II) Para o cumprimento de obrigação legal ou regulatória pelo controlador;
- III) Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
- IV) Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- V) Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- VI) Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
[...]
- VII) Para a proteção da vida ou da incolumidade física do titular ou de terceiro;

- VIII) Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- IX) Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;
- X) Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Existem diferentes tipos de leis de proteção de dados em vários países, com cláusulas de aplicação distintas umas das outras, porém as legislações baseadas na GDPR trazem similaridades em relação aos direitos dos titulares, que no caso do Brasil são sinalizados por nove incisos do Art 18º da lei nº 13.709:

- I) Confirmação da existência de tratamento;
- II) Acesso aos dados;
- III) Correção de dados incompletos, inexatos ou desatualizados;
- IV) Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
- [...]
- V) Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- VI) Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
- VII) Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- VIII) Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- IX) Revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

O Art 5º nos incisos VI a VIII da LGPD traz quem são as *personas* físicas capacitadas que têm o trabalho de gerenciar os dados pessoais, sendo eles os controladores, operadores e encarregados.

O controlador, segundo Lima (2020), pode ser uma pessoa natural ou jurídica, de direito público ou privado, na qual têm decisões relacionadas ao

tratamento dos dados, registros sobre o tratamento dos dados e comunicação com a ANPD. Estas decisões e procedimentos serão necessários para criar um plano operacional, sobre o que seguir para ficar de acordo com a LGPD.

Além de estar diretamente ligado ao titular dos dados, deve aplicar medidas de boas práticas, garantindo que as normas da LGPD estejam sendo seguidas.

O operador é quem desempenhará tarefas pré-definidas em nome do controlador, referente ao tratamento de dados, sempre documentando o mesmo e também, de acordo com o Art 39º, verificará a observância das próprias instruções e das normas sobre a matéria.

Já o cargo de encarregado, mais conhecido como *Data Protection Officer* (DPO), indicado pelo controlador, “[...] consiste em intermediar as ações entre o controlador, titulares de dados e a ANPD” (LIMA, 2020). O encarregado tem como tarefa defender os interesses do titular, ou seja, poderá entrar em contato com a Autoridade Nacional de Proteção de Dados caso ocorra algum tipo de infração ou irregularidades e se ambos os agentes estão cumprindo seus deveres.

Os agentes de tratamento devem seguir uma série de procedimentos para garantir a segurança dos dados pessoais, mesmo após o seu término, como é previsto no Art 47º.

Quando se trata de um risco iminente ou possível, em relação aos dados de alguém, é função do controlador entrar em contato com a ANPD e o titular das informações, conforme Art 48º.

Caso a ANPD não disponibilize os padrões técnicos mínimos, o cumprimento da LGPD deverá ser por meio da ISO/IEC 27000 que são padrões de boas práticas e segurança da informação necessários (BOTELHO, 2020), como citado no Art 49º:

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 e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

No *caput* do Art 50º é estabelecido que agentes de tratamento (controladores e operadores), podem estabelecer normas e regras de boas práticas, definindo as condições de organização, incluindo petições e reclamações de

titulares. As regras estabelecidas, em relação ao tratamento de dados, devem seguir o § 1º, que será levado em conta a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes do tratamento de dados do titular.

Para algumas leis é necessário um órgão público para educar, guiar e sancionar certos nichos da população, baseado em certa norma a que foi atribuído. No caso da LGPD não é diferente, como é descrito no Art 55º-A, é criada a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República, que deve ser o responsável pela aplicação e regulação da lei (MONTINI, 2020).

As sanções administrativas da LGPD entraram em vigor dia 14 de agosto de 2021, ou seja, desta data em diante, o órgão formado por indicações do Presidente da República, poderá aplicar punições aos agentes de tratamento de dados, podendo 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)

Com base na lei em questão, o presente trabalho visou acompanhar a implementação da LGPD em uma empresa do ramo de construção civil em Criciúma/SC, com mais de 30 (trinta) anos de atividade e pouco mais de 300 (trezentos) funcionários, e analisar os impactos decorrentes da lei.

2 MATERIAIS E MÉTODOS

Esta pesquisa é aplicada e de base tecnológica. A LGPD está sendo implementada na empresa com o auxílio de uma assessoria jurídica, da DPO eleita e de um comitê interno. Além das horas de trabalho, foram elaborados termos e normativos específicos relacionados a cada diretriz da lei.

2.1 PASSOS PARA IMPLEMENTAÇÃO

Com o estudo realizado, foi possível conhecer um pouco mais a LGPD, sua história e tudo que ela abrange, servindo de base para as próximas etapas que são necessárias para sua implementação em uma empresa. O processo se dá em várias etapas, desde a obtenção de informações a respeito do processo de coleta dos dados pessoais até a identificação de um *Data Protection Officer* (DPO).

Para realizar a implantação da LGPD na empresa, foi necessário conhecê-la bem, inclusive todos seus artigos e seções, principalmente quais são os tipos de dados de pessoa física que existem, quais pessoas serão os responsáveis para realizar o tratamento dos dados coletados e os treinamentos obrigatórios para os colaboradores.

A base teórica profunda, a respeito das legislações nacionais, está nos escritórios de advocacia, no qual é possível marcar reuniões prévias em relação a

LGPD, fornecendo assim a orientação inicial e os primeiros passos a serem realizados na empresa.

Outra fonte de conhecimento são cursos *online* ou presenciais com certificados renomados e de confiança, os quais a empresa pode inscrever colaboradores selecionados, para a futura coleta e tratamento dos dados pessoais, obtendo assim o conhecimento mínimo necessário para implementação da LGPD.

As diversas empresas no Brasil contêm rotinas ou *softwares* que utilizam dados de pessoa física em certo momento de seus processos. A etapa a seguir busca apontar algumas rotinas e necessidades de tratamento:

1. A coleta de informações ocorre, na maioria dos casos, no sistema de gestão integrado, mais conhecido como *Enterprise Resource Planning* (ERP) que grava inúmeros dados de colaboradores todos os dias sem as devidas cláusulas no contrato.
2. A utilização de *Business Intelligence* (BI) para produzir relatórios com vários tipos de dados contidos na empresa, podendo conter informações pessoais que não poderão ser utilizadas caso não haja consentimento do titular ou não tenha sido realizado a pseudo anonimização dos dados.
3. Sistema de monitoramento de câmeras, nas quais deverão ser revisadas para garantir que as imagens capturadas por elas estejam apenas dentro de sua propriedade, para a possível expansão do perímetro das imagens, é necessário verificar o subcapítulo referente aos requisitos para tratamento de dados.
4. Contratos com empresas parceiras que utilizam ou têm acesso a dados de seus colaboradores, necessitam, caso não possuam, cláusulas garantindo a segurança dos dados e qual o motivo de tal coleta ou transmissão.
5. A troca de informações pessoais, por meio de aplicativos de comunicação via telefone celular, é uma prática muito comum dentro das empresas, porém é difícil controlar os dados fornecidos, ou seja, sem os devidos termos e contratos assinados, torna-se inviável a utilização de tal tecnologia.

Para a devida utilização dos sistemas internos, foi necessário realizar o treinamento que a empresa oferece, mostrando assim que o colaborador está ciente em relação à LGPD e suas diretrizes. Se for levado em conta o pensamento de Neri (2020), a coleta do maior número possível de informações é de suma importância para a implementação da LGPD, garantindo assim maiores chances de sucesso no final da implantação na empresa.

A partir do momento que é realizada a coleta de algum tipo de dado de pessoa física, sendo pessoal ou sensível, a empresa se torna responsável por tal informação, com isso, podendo trazer riscos ao titular dos dados. O mapeamento de riscos para Batistella (2021) é formado por qualquer fator que de alguma maneira possa trazer riscos para a empresa, sendo eles pelo meio de trabalho, juridicamente ou riscos técnicos.

Ao coletar os dados para realização de certos serviços, é necessário mapear os riscos, no qual consiste em analisar as rotinas, desde a identificação dos dados até o momento de arquivamento ou deleção dos mesmos, que possam trazer riscos, tendo como base alguns critérios fornecidos por Batistella (2021): a) necessidade de retenção dos dados; b) enquadramento da coleta dos dados dentro de uma base legal; c) transparência na gestão do tratamento dos dados.

Um dos documentos mais importantes para a implementação da LGPD é o relatório de impacto, no qual é um dos componentes que foram herdados da GDPR, lei que regulamenta a proteção de dados na União Europeia na qual a LGPD é inspirada, sendo de grande ajuda para a empresa. Tal relatório, segundo o Art. 5º inciso XVII é uma documentação do controlador que descreve os processos (Figura 2) de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais. Consiste num documento que facilita a identificação dos riscos, a fim de minimizá-los.

Figura 2 – Etapas relatório de impacto



Fonte: Site [profissionaisti](#)

Com relação aos documentos internos e externos utilizados pelas empresas, segundo Neri (2020) deverão estar de acordo com todas as diretrizes da LGPD, respeitando o direito dos titulares e dos agentes de tratamento de dados. Para que tais documentos estejam acordados com a LGPD, foi necessária a criação de cláusulas adicionais, nas quais são citados quais dados serão coletados, por quanto tempo ficarão salvos no banco de dados e quais as bases legais utilizadas para dados pessoais e sensíveis.

Como a LGPD é um assunto consideravelmente novo para alguns brasileiros, esses não têm o conhecimento do que é um dado pessoal ou sensível, mesmo podendo ter acesso a eles em suas atividades. As empresas em *compliance* com a LGPD são obrigadas a realizar treinamentos específicos para cada setor que tenha acesso a dados de pessoa física, para que assim mude a cultura da empresa, relativo ao tratamento de dados pessoais, para que o projeto de adequação seja bem sucedido, e as mudanças implementadas sejam duradouras.

Os tipos de treinamento variam para cada setor, dependendo da quantidade de informações que este necessita para poder realizar seu trabalho, por exemplo, uma colaboradora dos Recursos Humanos (RH) terá de fazer mais treinamentos de tratamento de dados em relação a um operário de máquinas.

A definição de *compliance* para Rossetti e Pitta (2017, p. 42), “é um conjunto de ações que uma empresa deverá adotar para estar de acordo com certa legislação, prevenindo assim a ocorrência de infrações.” Para Frazão, Oliva e Abilio (2019, p. 694) “o *compliance* de dados tem como objetivo auxiliar os agentes de tratamento a aplicar, de forma eficaz, as normas de proteção de dados.”

“A necessidade de a empresa estar em *compliance* com a LGPD vem sendo um pré-requisito principalmente para um bom relacionamento interno, firmar boas relações externas e a ideologia que a empresa passará para o público.” (ROCHA; PONTINI, p.418).

Com base no estudo de *compliance* e suas principais finalidades descritas anteriormente, uma delas se destaca, qual seja, a necessidade de firmar boas relações externas com fornecedores, perante a LGPD.

Segundo Cavalcanti (2021), por mais que um fornecedor traga benefícios para quem o contratou para um tipo de serviço ou produto, mas não esteja de acordo com a LGPD, este apresenta riscos perante a nova lei, estes riscos podem aumentar caso seja fornecido algum tipo de dado de pessoa física. Caso seja detectada alguma irregularidade no tratamento de dados entre as empresas, seja por meio do DPO ou pela própria ANPD, ambas as empresas poderão sofrer as penalidades citadas no capítulo anterior.

Anteriormente foram abordados os agentes de tratamento de dados pessoais, sendo eles o controlador, operador e o encarregado, mais conhecido como *Data Protection Officer* (DPO). O DPO para Cruz (2021, p.22), “não é necessário ter algum tipo de graduação em sistemas de informação, porém é recomendado ter conhecimentos acerca da LGPD e estar devidamente informado em relação ao tratamento de dados.”

Dentre as atividades que o DPO realizará, são elas, conforme Art. 41º § 2:

- a) Adotar providências ao receber reclamações, comunicações dos titulares ou ao ser comunicado pela ANPD;
- b) Orientar colaboradores sobre as práticas em relação a proteção de dados;
- c) Executar atribuições determinadas pelo controlador.

3 RESULTADOS E DISCUSSÃO

Antes de realizar a implementação, foi necessário compreender a lei, sendo assim colaboradores do setor de RH, qualidade e o setor de informática, realizaram um curso de 10 (dez) horas relacionado à LGPD, no qual foi apresentada a lei e no que é baseada, quais seus propósitos, quais as penalidades e a partir de quando elas começariam. Após o treinamento foi conversado com a diretoria da empresa para informá-los desta nova lei, e o que poderia acontecer caso suas diretrizes não fossem seguidas. Feito isto, o diretor administrativo passou as

informações de contato da assessoria jurídica da empresa, para assim elaborar um plano de ação referente à LGPD.

Conforme conversado com os advogados, algumas dúvidas sobre a LGPD, a respeito dos procedimentos internos da empresa, foram esclarecidas, porém mais questionamentos surgiam, por isso foi criado um comitê interno para resolver as questões da LGPD e implementá-la na empresa.

Um dos passos mais importantes da implementação da LGPD foi selecionar uma pessoa para ser o encarregado de proteção de dados, mais conhecido como *Data Protection Officer* – DPO. Como a assessoria jurídica tem uma profissional capacitada e com alto conhecimento em relação à legislação de segurança da informação e privacidade de dados, foi definido-a como a DPO da empresa e assim fazendo parte do comitê interno.

O comitê interno foi composto por um representante de cada setor específico, sendo: recursos humanos, qualidade, segurança, expedição, comercial, dois representantes do setor de informática e o DPO. Ficou definido de ter, no mínimo, uma reunião mensal com este grupo para falar sobre o que foi implementado desde o último encontro e as próximas tarefas.

Os documentos são enviados pela DPO via *e-mail*, no qual contém um anexo de instruções de como proceder e a tarefa em si, que logo após recebido, define-se quem será o responsável por aquele documento e pelos trâmites dentro da plataforma Trello, alternando entre os quadros “Tarefas” que representa algo sem muita importância, “A Fazer” são prioridades, “Em Andamento” são as tarefas que estão sendo feitas e “Concluído” onde se encontram as tarefas finalizadas.

Uma das primeiras tarefas definidas foi a adequação do *site* da empresa conforme a LGPD. Foi contratada uma empresa para realizar a implementação do mínimo necessário previsto pela lei, que é o portal de privacidade no qual tem como objetivo possibilitar que o titular exerça seus direitos de forma facilitada. Está presente no portal o aviso de privacidade, aviso de *cookies*, solicitação de privacidade e os termos de uso. Os colaboradores, para continuarem trabalhando normalmente, tiveram de ser submetidos a um treinamento geral da LGPD instruído pela DPO, no qual foram divididos em três turmas em horários separados. A encarregada de dados apresentou si mesma, suas experiências profissionais na área de segurança de dados, explicou a lei e como poderia impactar a empresa.

A assessoria jurídica, junto do setor de recursos humanos, ficaram responsáveis pela revisão do novo contrato de colaboradores internos, adicionando novas cláusulas (Figura 3) e reformulando-o conforme a LGPD. O setor de informática ficou encarregado da coleta de assinaturas dos “Termos de Uso de Imagem” dos trabalhadores, no qual é citado que ao assinar o colaborador está autorizando a coleta gratuita de sua imagem, voz e som, e que o mesmo poderá ser divulgado nas redes sociais da empresa. O termo após assinado é anexado junto do contrato trabalhista do trabalhador, evitando assim perdas de documentos e facilidade na localização do mesmo. Foi realizado o levantamento inicial de quais são os prestadores de serviço externos para cada setor, para futuramente adequar seus respectivos contratos com a empresa.

Figura 3 – Novas cláusulas contratuais

Cláusula 14ª – O EMPREGADO pode optar por autorizar – ou não – o uso de sua imagem e voz em quaisquer veículos de comunicação a serem produzidos para a finalidade institucional, de marketing e comercial em território nacional e internacional. Para tanto, a imagem objeto da presente autorização poderá ser veiculada por todos os meios de divulgação, inclusive, mas não limitadamente, pela mídia impressa ou por transmissão eletrônica de dados (*online*), em folders de apresentação da entidade, folhetos, malas diretas, divulgação em reuniões, treinamentos, campanhas, vídeos, redes sociais, programa para rádio, entre outros, através dos quais todo e qualquer terceiro, cliente e/ou visitante, poderá ter acesso às mencionadas informações e imagem, cuja divulgação pública ora se autoriza, sendo difundida durante período indeterminado.

Parágrafo único: Por meio desta autorização ora concedida, autorizo, ainda a realizar nas imagens e sons captados, cortes, reduções e edições. Esta autorização não gera e não gerará no futuro e também não ensejará interpretação de existir quaisquer vínculos ou obrigações trabalhistas, securitárias, previdenciária, indenizatória ou mesmo empregatícia.

Parágrafo segundo: Esta autorização é feita a título gratuito, sem qualquer ônus à empresa, e tem validade enquanto houver uma permissão expressa minha. Podendo ser revogada, a qualquer tempo, de forma expressa (por escrito), mediante registro da solicitação.

Parágrafo terceiro. Com a revogação do consentimento, deixará de se tratar/ divulgar as imagens e sons à contar da requisição, sendo impossível eliminar as imagens de materiais e divulgações ocorridas durante o consentimento.

Foi elaborado e enviado, pela assessoria jurídica, um modelo da Política de Segurança da Informação (PSI), no qual o setor de informática adequou conforme as normas de acesso da empresa, contendo as responsabilidades dos usuários, políticas de utilização dos computadores e impressoras, permissões dentro da rede e as penalidades caso ocorra alguma infração da política. Foram adicionadas também normas complementares detalhando os processos e *softwares* internos, como a rotina de *backup*, normas de uso do aplicativo de comunicação

interna e *e-mail*, política de acesso remoto e a política de acesso à internet. Após a revisão do setor de informática e da assessoria, foi encaminhado a todos os colaboradores via *e-mail* a PSI, informando do que se tratava e que a leitura dela era obrigatória. Depois dos usuários conhecerem a política, foi realizado um treinamento para todos com acesso a rede sobre as boas práticas de uso da informação..

O setor de informática implementou em um sistema utilizado pelo setor Comercial e pelos Representantes externos, que é acessado por uma “*url*” de um *site*, uma aplicação no qual obriga o usuário a alterar a senha, no primeiro *login* após a atualização, para uma mais forte com alguns requisitos mínimos, tornando-o assim mais seguro e dificultando o acesso de usuários mal intencionados.

A comunicação é um fator chave para a LGPD, por isso foram criados dois canais de *e-mail*, um interno para colaboradores e outro externo para clientes e colaboradores rescindidos. O objetivo destes endereços eletrônicos é para os usuários citados anteriormente poderem tirar suas dúvidas referentes à LGPD, buscar informação se na empresa contém algum tipo de dado pessoal ou sensível armazenado e até mesmo pedir a exclusão dos mesmos, caso seja possível.

Foi criada a planilha de ativos e riscos (Figura 4, 5, 6) no qual tem como objetivo conhecer os ativos da empresa, assim como os riscos vinculados a cada um deles para posteriormente implementar medidas mitigatórias, diminuindo assim a possibilidade de incidentes em cada ativo. Nela foi necessário detalhar o processo executado em cada ativo, tipo de ativo, definir um grau (baixo, médio e alto) para três itens, a confidencialidade sendo a propriedade de que a informação ou dados pessoais não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados, a integridade como a propriedade de salvaguarda na exatidão e completude de ativos, garante que a informação não sofra alteração indevida, e a disponibilidade sendo a propriedade de estar acessível e utilizável quando demandada por uma entidade autorizada. Também devem ser relatados os controles já existentes dentro deste processo, quais as consequências caso venha a ocorrer um incidente e definir entre baixa, média e alta para a probabilidade e impacto, respectivamente, como probabilidade sendo a chance de ocorrer um incidente dentro deste processo e impacto é o grau de perigo caso ocorra algum incidente. Ao final da tabela, se encontram três colunas, o plano de tratamento, no qual se deve descrever quais medidas vão ser tomadas para melhorar o processo

descrito e logo após é necessário definir o grau de probabilidade e impacto novamente, porém contando após as medidas de proteção forem implementadas naquele processo.

Figura 4 – 1ª parte cabeçalho planilha de ativos e riscos

Processo	Ativo	C	I	D	Ameaça (genérica)	Ameaça (específica) (descreva como o evento pode acontecer, de que forma) Fatos: ocorrências no passado
----------	-------	---	---	---	-------------------	---

Figura 5 – 2ª parte cabeçalho planilha de ativos e riscos

Controles atuais existentes	Vulnerabilidade(s)	Consequências (Cenário do incidente e consequências aos ativos e processos de negócio. Valor financeiro (Reposição do ativo, operações suspensas/prejuízos) consequências da violação de segurança, mau uso das informações, violação de obrigações regulatórias/leis)	Probabilidade	Impacto
-----------------------------	--------------------	--	---------------	---------

Figura 6 – 3ª parte cabeçalho planilha de ativos e riscos

PLANO DE TRATAMENTO	NOVO PATAMAR DE RISCO	
Controles	Probabilidade	Impacto

Foi criada uma planilha para o controle de políticas, na qual são descritas quais políticas estão em vigor hoje na empresa, a data que foi criada e logo após a data para sua próxima revisão, variando de seis meses a dois anos. Esta planilha é de suma importância pelo fato da empresa, depois da implementação, ter criado um alto número de documentos, possibilitando a organização e o estabelecimento de prazos futuros para as políticas.

Será implementado o plano de conscientização de colaboradores, parceiros e fornecedores, no qual consiste num documento com ações a serem tomadas, como alguns treinamentos, comunicados e campanhas relacionados a dúvidas referentes à LGPD, segurança da informação e algumas sugestões de leitura. Está pendente também a solicitação de orçamento das fragmentadoras de papéis, utilizadas para o descarte seguro dos documentos conforme a norma DIN 66399, no qual estabelece requisitos mínimos para a destruição de documentos ou mídias.

Será enviado também aos representantes comerciais da empresa um modelo do termo de consentimento que deverá ser repassado para seus clientes, do tipo pessoa física, constando quais dados serão captados pela empresa.

4 CONCLUSÃO

No presente trabalho foi acompanhado a implementação parcial da LGPD em uma empresa do ramo de construção civil em Criciúma/SC. A lei, por ser extensa e relativamente nova, gerou muitas dúvidas em cenários específicos da empresa mesmo após ser compreendida, já que não existe muito referencial teórico nacional relacionado à implementação em empresas, porém com o auxílio da assessoria jurídica e da DPO, os questionamentos foram sendo resolvidos e a implementação se fez possível.

Após compreender a LGPD e suas dificuldades, foram identificados os tipos de dados de pessoa física que necessitam de tratamento, sendo eles pessoais (CPF, RG, nome completo, telefone, *e-mail*, endereço, número do SUS, matrícula dentro da empresa, etc...) e sensíveis (opção religiosa, dado genético e referente a saúde ou sexualidade, filiação sindical, opinião política, origem racial).

Após muitas reuniões e revisões entre o setor de RH e a assessoria jurídica, os contratos internos foram adequados conforme a LGPD, adicionando cláusulas de acordo com a lei mencionadas no capítulo anterior. Os contratos externos ainda não foram analisados, pelo fato de que não foi finalizado o levantamento dos operadores de dados da empresa.

Devido o prazo ter sido curto para a implementação total da LGPD na empresa, não foi possível finalizá-la por completo, ficando assim algumas pendências para serem feitas, como os treinamentos específicos para cada setor que ainda serão realizados conforme cronograma da implementação.

Tendo em vista, que cada empresa tem as prioridades definidas conforme as necessidades, com a LGPD não foi diferente, algumas atividades prioritárias acabaram sendo executadas antes do cronograma da implementação, atrasando-a e fazendo com que não fosse completada a implementação até a presente data. Em virtude do alto número de documentos que foram gerados, como a política de segurança da informação, a planilha de ativos e riscos que consta todos os ativos e

informações referentes a dado pessoal e sensível dentro da empresa, junto de alguns questionários, é possível afirmar que implementar a LGPD numa empresa demandou muito tempo para ler, compreender e repassar as informações de cada documento aos outros colaboradores. Um dos pontos mais difíceis da implementação na empresa foi a mudança de hábitos e rotinas dos colaboradores, fazê-los se acostumar com “novas” boas práticas, como por exemplo, bloquear a tela do *Windows* ao sair de perto do computador, não compartilhar imagens de colaboradores em grupos da empresa em redes sociais e deixar documentos com dados pessoais em lugares de fácil acesso.

Até o fim do presente trabalho não foi possível verificar algum tipo de avanço imediato pelos funcionários ou clientes após a implementação da LGPD na empresa.

Para trabalhos futuros recomenda-se a busca de referencial teórico acerca da implementação da GDPR em empresas na União Europeia, devido ao fato da LGPD ter como base essa lei e a escassez desse conteúdo em território brasileiro.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (Brasil). **NBR 6023**: Informação e documentação - Referências - Elaboração. Rio de Janeiro: ABNT, 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (Brasil). **NBR 6024**: Informação e documentação - Numeração progressiva das seções de um documento escrito - Apresentação. Rio de Janeiro: ABNT, 2003.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (Brasil). **NBR 6028**: Informação e documentação - Resumo - Apresentação. Rio de Janeiro: ABNT, 2003.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (Brasil). **NBR 10520**: Informação e documentação - Apresentação de citações em documentos. Rio de Janeiro: ABNT, 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (Brasil). **NBR 14724**: Informação e documentação - Trabalhos acadêmicos - Apresentação. Rio de Janeiro: ABNT, 2011.

BATISTELLA, Carla. **Mapeamento de riscos na área de TI e adequação à LGPD**. Disponível em: <https://www.certifiquei.com.br/mapeamento-riscos/>. Acesso em: 01 jun. 2021.

CAVALCANTI, Leo. **LGPD de fornecedores: 4 maneiras de reduzir os riscos na sua empresa. 4 maneiras de reduzir os riscos na sua empresa.** 2021. Disponível em: <https://www.linkana.com/blog/lgpd-fornecedores/>. Acesso em: 10 jun. 2021.

BOTELHO, Marcos César. **A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes.** Revista Direitos Sociais e Políticas Públicas – Unifafibe. V. 8, N. 2, 2020.

BRASIL, Hsc. **O que é GDPR e o que muda para as empresas e os brasileiros?** Disponível em: <https://www.hscbrasil.com.br/gdpr/>. Acesso em: 18 maio 2021.

BRASIL. Lei 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, ago. 2018.

BU, Fei *et al.* **“Privacy by Design” implementation: information system engineers perspective.** Amsterdã: Elsevier, 2020. 53 v.

CÂMARA, Flávia da Silva. **Lei geral de proteção de dados pessoais (LGPD) – aplicada às empresas de contabilidade.** [s.l.: s.n., s.d.]. Disponível em: <https://monografias.ufrn.br/jspui/bitstream/123456789/10702/1/LeiGeraldeProtecao_Camara_2020.pdf>. Acesso em: 26 nov. de 2020.

CARVALHO, Thaís Abreu. **Aplicabilidade da lei geral de proteção de dados e da metodologia privacy by design nos termos de uso e de política de privacidade.** 2019. 61 f. TCC (Graduação) - Curso de Direito, Faculdade de Direito de Vitória Curso de Graduação em Direito, Vitória, 2019.

CAVOUKIAN, Ann. **Information & Privacy: 7 foundational principles.** Internet Architecture Board. 2011. Disponível em: https://www.iab.org/wpcontent/IABuploads/2011/03/fred_carter.pdf. Acesso em 18 out. 2019.

CÉSAR, Ana Carolina Moreira; ASPIS, Fábio Lara; CHAVES, Luis Fernando Prado. **1 ano da GDPR: o que podemos aprender com os erros e acertos da Europa.** 2019. Disponível em: <https://www.conjur.com.br/2019-mai-31/opiniao-podemos-aprender-europa-ano-gdpr>. Acesso em: 14 jun. 2021.

COHEN, Renato. **Performance como linguagem.** 3. ed. São Paulo: Perspectiva, 2013.

CRUZ, Danielle da Costa Santos. **A Lei Geral de Proteção de Dados Pessoais (LGPD): contribuições sobre o uso e proteção de dados para as instituições de ensino. contribuições sobre o uso e proteção de dados para as instituições de ensino.** 2021. Disponível em: <bdta.ufra.edu.br/jspui/handle/123456789/1711>. Acesso em: 08 jun. 2021.

FERNANDES, Celso; *et al.* **Coordenação geral enciclopédia jurídica da PUCSP tomo 2 direito administrativo e constitucional coordenação do tomo 2.** [s.l.: s.n.,

s.d.]. Disponível em: <https://enciclopediajuridica.pucsp.br/pdfs/direito-a-privacidade_58e9502c41f94.pdf>. Acesso em: 26 nov. de 2020.

GOLDMAN, Eric. **An Introduction to the California Consumer Privacy Act (CCPA)**. 2020. 7 f. Tese (Doutorado) - Curso de Direito, Santa Clara University School Of Law, Santa Clara, 2020.
<http://app.fiepr.org.br/revistacientifica/index.php/conhecimentointerativo/article/view/499>

GOMES, Maria Cecília Oliveira. **Relatório de impacto à proteção de dados**. Revista do Advogado, São Paulo, n. 144, p. 174-183, 2019.

IGBE. **Pesquisa mostra que 82,7% dos domicílios brasileiros têm acesso à internet**. Disponível em: [https://www.gov.br/mcom/pt-br/noticias/2021/abril/pesquisa-mostra-que-82-7-dos-domicilios-brasileiros-tem-acesso-a-internet#:~:text=Em%202019%2C%20entre%20as%20183,estudantes%20\(75%2C8%25\)..](https://www.gov.br/mcom/pt-br/noticias/2021/abril/pesquisa-mostra-que-82-7-dos-domicilios-brasileiros-tem-acesso-a-internet#:~:text=Em%202019%2C%20entre%20as%20183,estudantes%20(75%2C8%25)..) Acesso em: 14 jun. 2021.

LIMA, Victor Henrique Pereira. **IGPD análise dos impactos da implementação em ambientes corporativos: estudo de caso**. 2021. 43 f. TCC (Graduação) - Curso de Ciência da Computação, Pontifícia Universidade Católica de Goiás, Goiânia, 2020.

LIMA, Cíntia Rosa Pereira de; PEROLI, Kelvin. A governança e as boas práticas no sistema de proteção de dados pessoais do Brasil. **Anais do III Encontro de Pesquisa e Iniciação Científica da Universidade Metropolitana de Santos**, p. 98.

NERI, Leonardo. **LGPD – AS FASES DE IMPLEMENTAÇÃO DE UM PROGRAMA DE PRIVACIDADE**. Disponível em: <https://www.mazzuccoemello.com/igpd-as-fases-de-implementacao-de-um-programa-de-privacidade/>. Acesso em: 31 maio 2021.

OLIVEIRA, Gabriel Prado Souza de. **Sigilo de Dados no Brasil: da Previsão Constitucional à Nova Lei Geral De Proteção De Dados Pessoais - Âmbito Jurídico**. Âmbito Jurídico. São Paulo, 01 de fev. de 2020. Disponível em: <<https://ambitojuridico.com.br/cadernos/direito-constitucional/sigilo-de-dados-no-brasil-da-previsao-constitucional-a-nova-lei-geral-de-protacao-de-dados-pessoais/#:~:text=De%20acordo%20com%20o%20art,ou%20%C3%A0%20vida%20sexual%20etc>>. Acesso em: 26 nov. de 2020.

PARTHASARATHY, A. (2020). Coronavirus challenge: Propelling a new paradigm of work from home. **Science Reporter**, 57(4), 14-19

PRIVACY ACT OF 1974. Disponível em: <https://www.justice.gov/opcl/privacy-act-1974>. Acesso em: 20 maio 2021

RAMOS, P. A regulação de proteção de dados e seu impacto para a publicidade online: um guia para a LGPD. **Baptista Luz**, 16 jul 2019. Disponível em: <https://baptistaluz.com.br/institucional/a-regulacao-de-protacao-de-dados-e-seu-impacto-paraa-publicidade-online-um-guia-para-a-igpd/>. Acesso em: 18 maio 2021.

RODOVALHO, João Paulo. **Proteção de dados pessoais nas relações de emprego: a prevenção da empresa depois da LGPD**. Google Books. Disponível em: <https://books.google.com.br/books?id=IToKEAAAQBAJ&pg=PA86&dq=dados+sensíveis&hl=pt-BR&sa=X&ved=2ahUKEwiNx4rktP7tAhXMJrkGHR_wAE4Q6AEwAXoECAAAQAg#v=onepage&q&f=false>. Acesso em: 26 nov. de 2020.

ROCHA, Cláudio Jannotti da; PONTINI, Milena Souza. Compliance trabalhista: impacto da lei geral de proteção de dados (lgpd) no direito do trabalho. Lisboa: **Revista Jurídica Luso Brasileira**. 04 fev. 2021.

ROJAS, Marco Antonio Torrez. **Avaliação da adequação do Instituto Federal de Santa Catarina à Lei Geral de Proteção de Dados Pessoais**. 2020. Disponível em: <https://repositorio.ifsc.edu.br/handle/123456789/1433>. Acesso em: 08 jun. 2021.

ROSSETTI, Maristela Abla; PITTA, Andre Grunspun. **Governança Corporativa: avanços e retrocessos**. São Paulo: Quarter Latin do Brasil, 2017

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

SILVEIRA SOBRINHO, Nayara da. **A proteção de dados pessoais no e-commerce: análise da aplicação da lgpd diante da vulnerabilidade do consumidor**. 2019. 52 f. Tese (Doutorado) - Curso de Direito, Centro Universitário Unifacig, Manhauçu, 2021.

TEDEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Revista dos Tribunais, 2019.

TEFFÉ, C. S. DE; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **civilistica.com**, v. 9, n. 1, p. 1-38, 9 maio 2020.

DODT, Cláudio. **LGPD: Como criar um RIPDP – Relatório de Impacto à Proteção de Dados Pessoais**. Disponível em: <https://www.linkana.com/blog/igpd-fornecedores/>. Acesso em: 08 dez. 2021.