INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIAS E TECNOLOGIA DO AMAZONAS CAMPUS MANAUS CENTRO DEPARTAMENTO ACADÊMICO DE INFORMAÇÃO E COMUNICAÇÃO CURSO SUPERIOR DE TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

Eduardo Matheus Rodrigues Da Silva

Gerador Do Inventário De Dados Pessoais e do Relatório de Impacto à Proteção De Dados

Manaus-2022
AM

Eduardo Matheus Rodrigues Da Silva

Gerador Do Inventário De Dados Pessoais e do Relatório de Impacto à Geração De Dados

Trabalho de Conclusão de Curso apresentado a banca examinadora do Curso de Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Amazonas, como requisito para aprovação na disciplina TCC 2 – Desenvolvimento de Software.

Orientador:Prof Dr Renildo Viana Azevedo

Manaus-2022
AM

Biblioteca do IFAM – Campus Manaus Centro

S586g Silva, Eduardo Matheus Rodrigues da.
Gerador do inventário de dados pessoais e do relatório de impacto à proteção de dados / Eduardo Matheus Rodrigues da Silva. – Manaus, 2022.
60 p. : il. color.

Trabalho de Conclusão de Curso (Tecnologia em Análise e Desenvolvimento de Sistema) – Instituto Federal de Educação, Ciência e Tecnologia do Amazonas, *Campus* Manaus Centro, 2022.
Orientador: Prof. Dr. Renildo Viana Azevedo.

1. Desenvolvimento de sistema. 2. Gerador de inventário. 3. Impacto à proteção de dados. I. Azevedo, Renildo Viana. (Orient.) II. Instituto Federal de Educação, Ciência e Tecnologia do Amazonas III. Título.

CDD 005.3

Elaborada por Márcia Auzier CRB 11/597

Eduardo Matheus Rodrigues Da Silva

Gerador Do Inventário De Dados Pessoais e do Relatório de Impacto à Geração De Dados

Trabalho de Conclusão de Curso apresentado a banca examinadora do Curso de Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia do Amazonas, como requisito para aprovação na disciplina TCC 2 – Desenvolvimento de Software.

Orientador:Prof Dr Renildo Viana Azevedo

Aprovado em_____de_____de 2022

BANCA EXAMINADORA

_____

Prof. Dr Renildo Viana Azevedo (orientador)
Instituto Federal do Amazonas

_____

Profa Dra Viviane Gomes da Silva
Instituto Federal do Amazonas

_____

Professor MSc Paulo Henrique de Lima Maciel
Instituto Federal do Amazonas

Manaus-2022
AM

Agradecimentos

Agradeço a Deus que me permitiu tudo isso, a minha família e amigos que sempre me apoiaram em vários momentos da minha vida, a instituição que mostrou o caminho e abriu várias oportunidades e onde conheci ótimas pessoas na qual aprendi muito com elas a evoluir tanto profissionalmente como ser humano.

Agradeço ao Professor Renildo Viana, pelas preciosas dicas e orientações que aperfeiçoaram este trabalho.

RESUMO

O objetivo deste trabalho é desenvolver um sistema web para o tratamento de dados pessoais de acordo com a Lei nº 13.709 que corresponde à Lei Geral de Proteção de Dados (LGPD) determina, para automatizar a criação do Inventário de Dados Pessoais - IDP e o Relatório de Impacto à Proteção de Dados (RIPD), que representar importantes documentos de governança de dados pessoais e subsídio para avaliação de impacto sobre a proteção de dados pessoais, a fim de verificar o cumprimento pela instituição do que é recomendado pela LGPD.

Palavras-chave: LGPD, Dados, Inventário de Dados Pessoais, Relatório de Impacto à Proteção de Dados (RIPD), empresas

ABSTRACT

The objective of this work is to develop a web system for the processing of personal data in accordance with Law No. 13.709 which corresponds to the General Data Protection Law (LGPD) determines, to automate the creation of the Personal Data Inventory - IDP and the Report of Impact on Data Protection (RIPD), which represent important documents of governance of personal data and subsidy for impact assessment on the protection of personal data, in order to verify the institution's compliance with what is recommended by the LGPD.

Keywords: LGPD, Data, Personal Data Inventory, Data Protection Impact Report (RIPD), companies

Sumario

INTRODUÇÃO 9

PROBLEMATIZAÇÃO 12

JUSTIFICATIVA 13

OBJETIVOS 15

Objetivo Geral 15

Objetivo Específico 16

METODOLOGIA. 16

AS RAZÕES PARA A CRIAÇÃO DA LEI DE PROTEÇÃO A DADOS PESSOAIS 17

Lei Carolina Dieckmann 19

Escândalo Cambridge Analytica 21

Lei de Proteção de Dados- LGPD 22

FERRAMENTAS UTILIZADAS NO DESENVOLVIMENTO DA APLICAÇÃO E SISTEMAS CORRELATOS 28

FERRAMENTAS E TECNOLOGIA 29

HTML 5 29

CSS 29

JavaScript 30

Bootstrap 31

Thymeleaf 31

Java 32

Spring Boot 33

Hibernate 38

MySQL 39

DESENVOLVIMENTO DA APLICAÇÃO 40

Inventário de Dados 40

Relatório de Impacto à Proteção de Dados (RIPD) 43

DIAGRAMA DE CASOS DE USO 46

Descrição do Caso De Uso 46

Diagrama De Classes 55

Considerações Finais ____ *56*
REFERÊNCIAS ____ *57*

INTRODUÇÃO

Desde 1969 quando a internet foi criada e até os dias atuais, essa ferramenta modificou todos os âmbitos da existência humana, desde a comunicação até a forma de se fazer negócios. Dessa forma as relações pessoais mudaram, com isso surgem novos tipos de crimes. A legislação brasileira não cobre por completo todos os atos feitos em ambiente virtual. Por conta disso, as autoridades brasileiras perceberam a necessidade de regulamentações para a proteção dos dados de pessoas usuárias na rede.

A primeira lei com a preocupação com dados pessoais surgiu na Alemanha, na década de 1970. Com o avanço da industrialização e da computação nos países desenvolvidos, impulsionou a Alemanha a criar normas para regular a privacidade no país. Essa foi a primeira vez que o conceito de proteção de dados seria introduzido no cenário jurídico da Alemanha. Embora o conceito tenha sido desenvolvido desde o início da década de 1970, a legislação foi finalizada e implementada em 1978. Países como França, Noruega, Suécia e Áustria também criaram em 1978 suas próprias leis sobre como as informações de seus cidadãos poderiam ser utilizadas.

A Constituição brasileira de 1988 já mencionava alguns pontos sobre a proteção de dados. O artigo 5º da Constituição, referente aos Direitos e Deveres dos Cidadãos, já tratava, de forma geral, da privacidade dos cidadãos brasileiros: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. A lei 9.296 criada em 1996 acrescentou que é “inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal”.

O Código De Defesa do consumidor brasileiro possui uma parte sobre a defesa de informação que é a parte específica a respeito do cadastro e banco de dados. No texto da legis-

lação e defendido o direito do consumidor acessar os dados que uma empresa tem sobre ele e solicitar sua correção, caso alguma informação esteja incorreta. O artigo 11 garante a privacidade e responsabiliza as empresas sobre a segurança dos dados ,de acordo com o artigo 11 do Decreto nº 6.523 de 31 de Julho de 2008, "Os dados pessoais do consumidor serão preservados, mantidos em sigilo e utilizados exclusivamente para os fins do atendimento", e no artigo 13 ainda deixa claro que dificultar o acesso às suas próprias informações ou deixar de comunicar ao titular sobre o registro de seus dados são consideradas infrações.

O Parlamento Europeu e o Conselho da União Europeia criaram o regulamento 95/46/CE que estabelecia regras para serem cumpridas por todos os países da União Europeia (EU). Formalmente foi aprovado em 24 de outubro de 1995, para entrar em vigor três anos depois. A diretiva é um amplo texto legal em matéria de proteção de dados pessoais, determina que cada país membro tivesse um órgão ou profissional responsável pela supervisão e implementação e adequassem suas leis regionais para estar em conformidade com a 95/46/CE.

Em 2000 a Europa e os Estados Unidos estabeleceram um acordo para facilitar a troca de informações e dados pessoais entre os dois pólos. Em 2015 esse acordo foi revogado por suspeitas de espionagem por parte da Agência de Segurança Nacional dos EUA, porém, no ano seguinte, a Europa aprovou o "*Privacy Shield*", um novo programa de transferência internacional de dados com empresas norte-americanas que garantia maior segurança para os cidadãos europeus.

No Brasil em março de 2013 o decreto nº 7.962 acrescentou algumas orientações que complementam o Código de Defesa do Consumido. O artigo 2º define que são diretrizes do Plano Nacional de Consumo e Cidadania a "autodeterminação, privacidade, confidencialidade e segurança das informações e dados pessoais prestados ou coletados, inclusive por meio eletrônico". Em 25 de março de 2014 na câmara dos deputados e no Senado Federal em 23 de abril de 2014 foi aprovado a lei n°12.965/2014 conhecida como Marco Civil, que foi sancionada pela então presidente Dilma Rousseff, foi a primeira lei responsável por regular o uso da internet, no qual foram introduzidos conceitos como a neutralidade de rede e a liberdade de expressão e definidas quais são as obrigações dos órgãos públicos no fornecimento de internet.

Com o surgimento de casos de grande vazamento de dados e a comercialização de informações pessoais, a União Europeia decidiu alterar suas regras de proteção de dados surgindo a GDPR General Data Protection Regulation, a lei obriga empresas de todo mundo, inclusive gigantes como o Meta e o Google, a mudar a forma como coletam e tratam dados e foi responsável por uma nova onda de leis sobre o tema em todo o mundo, inclusive no Brasil, pois contém cláusulas e exigências relativas à forma como são tratadas informações pessoais na União Europeia, é aplicável a todas as empresas que operem no Espaço Económico Europeu, independentemente do seu país de origem, o regulamento não permite o tratamento de quaisquer dados fora do contexto legal especificado no regulamento, exceto no caso em que quem controla os dados tenha recebido consentimento explícito do proprietário dos dados. O proprietário tem ainda o direito de revogar essa permissão em qualquer momento.

Com a criação da GDPR General Data Protection Regulation, que é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia, e Espaço Económico Europeu, entrou em vigor no ano de 2018, ela inspirou outros continentes e países a tomarem caminhos semelhantes, em agosto de 2018 e inscrita sob o número 13.709 a versão brasileira da lei europeia, a LGPD que é uma lei que busca garantir a segurança de dados pessoais, respeitando a liberdade individual e a privacidade de cada, com isso ficou muito fácil combater os crimes virtuais que, seguindo o ritmo do resto do mundo, tiveram um crescimento vertiginoso nos últimos anos.

Em setembro de 2020 no Brasil por conta da pandemia do novo coronavírus a LGPD estava em funcionamento em caráter educativo, porém em 1 de agosto de 2021 entrou em funcionamento, isso significou que empresas, que não se adequaram às suas diretrizes que incluem desde informar ao usuário o motivo da coleta de dados específicos sobre ele até a proteção dessas informações poderão sofrer sanções judiciais.

As sanções judiciais, nesse sentido, podem adquirir a forma de qualquer penalidade de âmbito cível aplicável pelo Judiciário. Nessa categoria, estão incluídas as indenizações por danos materiais e morais; as reparações consumeristas em geral, vinculadas ao Código de Defesa do Consumidor; as obrigações de adequação da atividade da empresa, vinculadas a multas simples ou diárias; entre outras.

No dia 8 de julho de 2019, o presidente Jair Bolsonaro sancionou o texto que prevê a criação da Autoridade Nacional de Proteção de Dados (ANPD), surgindo assim a Lei nº 13.853,

criação dessa autoridade nacional independente para fiscalizar o cumprimento da LGPD faz com que o Brasil esteja de acordo com o Regulamento Geral sobre a Proteção de Dados da União Europeia, o que torna o país capacitado para a negociação de dados pessoais com países da Europa. A Autoridade Nacional de Proteção de Dados (ANPD) é composta por um Conselho Diretor, que é o órgão máximo de direção, um conselho nacional de proteção de dados pessoais e da privacidade, corregedoria, ouvidoria, um órgão de assessoramento jurídico próprio e unidades administrativas e unidades especializadas necessárias à aplicação da LGPD.

As punições que foram determinadas em dezembro de 2019, são a suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de seis meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador, a suspensão do exercício da atividade de tratamento dos dados pessoais, também pelo período máximo de seis meses, prorrogável pelo mesmo período; e a proibição parcial ou total do exercício de atividade relacionadas a tratamento de dados.

A LGPD menciona diversas obrigações da empresa durante o tratamento dos dados pessoais. Se a empresa, em razão do exercício de atividade de tratamento de dados pessoais, causar dano material ou moral, individual ou coletivo será obrigada a repará-lo.

PROBLEMATIZAÇÃO

A lei da LGPD lei de proteção de dados afetou completamente a forma como as empresas que operam no Brasil lidam com informações e dados pessoais, às empresas que não se adequarem, poderão ser aplicadas diversas sanções, desde advertência, para casos menos graves, até multas que podem chegar a 2% do faturamento do negócio, desde que não ultrapasse o teto de R$ 50 milhões.

Foi realizado uma pesquisa pela Fundação Dom Cabral (FDC) revelou que, das 207 empresas entrevistadas, 40% reconheceram não estarem plenamente adequadas à legislação, as empresas pertencem a segmentos distintos como finanças, seguros, varejo, agronegócio, saúde, química e construção, sendo de médio e grande porte. Idealizado e liderado pelos professores Dalton Sardenberg e Fernando Santiago, o levantamento foi realizado no primeiro semestre de 2021. Chamado de "A LGPD nas empresas dotadas de conselho de administração e conselho consultivo".

Ainda que exista uma quantidade elevada de companhias despreparadas para atender a LGPD, a pesquisa revela que 82% delas consideram que a adequação à Lei é total ou parcialmente uma das principais prioridades para até o fim 2021, 66% já nomearam um Encarregado pela Proteção dos Dados Pessoais (ETD), figura também conhecido como *Data Protection Officer (DPO)*, pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

As empresas que capturam os dados dos clientes (nome, telefone, e-mail, CPF, entre outros) e utilizam essas informações, por exemplo, para ações de publicidade, como envio de promoções pelo WhatsApp, precisam passar por um Programa de Adequações. Divulgação de listas com dados de clientes ou até mesmo envio de propaganda relacionadas às compras em determinado estabelecimento deve ser aplicado a lei. O tratamento irregular pode levar à aplicação de sanções civis e administrativas previstas na LGPD bem como outras sanções previstas em outras leis, como o CDC, o Código Civil e o Código Penal.

Para se adequarem as empresas precisam elaborar dois documentos, um documento conhecido como Inventário de Dados Pessoais - IDP que é a forma principal para documentar o tratamento de dados pessoais realizados pela instituição em alinhamento ao previsto pelo art. 37 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), a maioria das empresas possuem a obrigação de criar esse documento. O outro documento é o Relatório de Impacto à Proteção dos Dados Pessoais (**RIPD**), é um documento que demonstra os riscos nas operações de tratamento de dados pessoais.

O setor privado é obrigado a controlar seus tratamentos pessoais, e devem prestar esclarecimento à ANPD, eles são obrigados a saber os riscos do procedimento de dados, isso é complexo demais para ser controlado manualmente.

JUSTIFICATIVA

No Brasil, a LGPD (Lei nº 13.709, de 14/8/2018) entrou em vigor em 18 de setembro de 2020, representando um passo importante para a proteção de dados no Brasil. Com isso, passamos a fazer parte de um grupo de países que contam com uma legislação específica para

a proteção de dados dos seus cidadãos. Diante dos atuais casos de uso indevido, comercialização e vazamento de dados como escândalo envolvendo o Meta e a empresa britânica "*Cambridge Analytica*" deu início à discussão mundial sobre o uso indevido de dados de usuários em redes sociais. As novas regras são ferramentas para garantir a privacidade dos brasileiros, além de evitar entraves comerciais com outros países.

A LGPD quando foi aprovada no Brasil, criou um órgão da administração pública que faz parte da Presidência da República e possui atribuições relacionadas à proteção de dados pessoais e da privacidade, conhecido como a Autoridade Nacional de Proteção de Dados (ANPD). A ANPD determinou que as empresas que trabalham com dados no Brasil possuem a obrigação de criar dois documentos: o Inventário de Dados Pessoais (IDP) e o Relatório de Impacto à Proteção de Dados (RIPD).

O inventário de dados refere-se a um documento essencial quando estamos no processo de adequação às normas de proteção de dados, no caso do Brasil a LGPD, é um documento ou uma planilha que deve mostrar o caminho que o dado pessoal da empresa e procedimentos, processos pelo qual o dado percorrer. O documento mostra um panorama geral de como a empresa está lidando com a questão da privacidade e segurança da informação.

Os principais objetivos do Inventário de Dados Pessoais (IDP) é identificar a forma como a empresa lida com a privacidade e a segurança da informação de seus clientes, colaboradores e parceiros terceirizados, cumprindo, desta forma, a exigência constante no art. 37 da LGPD em qual estipula que o controlador, que é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, e o operador que é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, devem manter registros das operações de tratamento de dados pessoais.

O Relatório de Impacto à Proteção de Dados (RIPD) é focado nos direitos dos indivíduos, de forma que: 1) o conceito do relatório de impacto prevê a elaboração desse instrumento quando as atividades puderem gerar "riscos às liberdades civis e aos direitos fundamentais" (artigo 5º, XVII, LGPD); e 2) entre as competências da Autoridade Nacional de Proteção de Dados (ANPD) está regulamentar o RIPD para os casos em que o tratamento representa "alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na lei" (artigo 55-J, XIII, LGPD).

O Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) é um documento que o controlador tem a responsabilidade da elaboração, cumpre a função de demonstrar como os dados pessoais são coletados, tratados, usados, compartilhados e quais medidas são adotadas para diminuição dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados, ou seja constitui uma ferramenta de gestão de riscos à privacidade.

O sistema web que esse trabalho propõe, tem como finalidade facilitar a criação dos documentos, Relatório de Impacto à Proteção dos Dados Pessoais (RIPD), e o Inventário de Dados Pessoais (IDP), é possível criar esses documentos manualmente, contudo é mais trabalhoso pois será necessário criar planilhas e fora a dificuldade de manter uma plena organização, ou seja é vantajoso utilizar uma ferramenta automatizada e mais rápida e fácil.

As complexidades de se usar o IDP manualmente são devidas as seguintes questões, as inúmeras informações coletadas, e de segurança, todavia que podem ocorrer incidentes com os documentos. O RIPD é um documento de relevante e fazê-lo manualmente se têm probabilidades maiores de incidentes que em determinada medida pode causar danos financeiros e sanções com o órgão Autoridade Nacional De Proteção de Dados (ANPD).

OBJETIVOS

Objetivo Geral

Desenvolver uma aplicação web para auxiliar empresas e órgãos públicos no inventário de dados em qual estão alocados os registros de todas as operações de tratamento de dados, e no RIPD, uma documentação que descreve os processos de tratamento de dados pessoais que podem gerar algum risco aos direitos dos titulares, além das medidas e mecanismos empregados para mitigar esses riscos.

Objetivo Específico

- Definir os requisitos de uma RIPD e da IDP;
- Desenvolver processos para o inventário de dados web;
- Desenvolver funcionalidades automatizado para Relatório de Impacto à Proteção dos Dados Pessoais (RIPD);

METODOLOGIA**.**

Para a resolução dos problemas encontrados primeiramente foram levantados alguns requisitos para a criação de um novo sistema e como o mesmo poderia ser utilizado pelas empresas, em sequência foi projetado uma ideia de solução, e que por final foi executado e aplicado na organização.

O presente trabalho, pode ser classificado como uma pesquisa Revisão de Literatura, pois resume toda a informação existente, da forma mais completa possível. Do ponto de vista técnico esse trabalho pode ser classificado como um estudo de caso.

Os métodos utilizados para realizar uma pesquisa estão diretamente ligados ao problema a ser estudado e a escolha da metodologia de maneira direta dos objetivos do projeto. O objetivo deste trabalho é criar uma ferramenta online na qual facilite a criação dos relatórios que pela lei de proteção de dados as empresas e órgãos públicos que trabalhem com dados, são obrigados a fazer.

A metodologia utilizada nesta pesquisa, para o desenvolvimento deste projeto, foi o levantamento bibliográfico, por meio de inúmeras fontes foram examinados artigos, trabalhos acadêmicos, reportagens e a própria Lei n. 13.709, a leitura e fichamento do referencial teórico,

o estudo das ferramentas de desenvolvimento da aplicação, é por fim o desenvolvimento do projeto.

AS RAZÕES PARA A CRIAÇÃO DA LEI DE PROTEÇÃO A DADOS PESSOAIS

Em reconhecimento ao direito de proteger a vida privada como um direito humano, 1948 Declaração Universal dos Direitos Humanos - Adotada pela Assembleia Geral da ONU As Nações Unidas e reconhecendo a necessária proteção da privacidade, As pessoas e famílias, nos termos do artigo 12 e da liberdade de informação, opinião e expressão, De acordo com o Artigo 19 (Organização das Nações Unidas, 1948)— Objeto das mais diversas reflexões, sobretudo quando onipresente Confirme que os dados pessoais são uma nova mercadoria (DONEDA, 2006, p. 372). "Não é à toa que se fala em "morte da privacidade", crise ou erosão da intimidade, pois a realidade que lhe é subjacente demonstra que os dados pessoais são o que alimenta e movimenta tal economia é, mais do que isso, são a base de sustentação e ativo estratégico de uma série de modelos de negócios e para formulação de políticas públicas. Há uma economia 254 e uma sociedade que são cada vez mais reféns e dependentes desse livre fluxo informativo" (Bioni, 2019, p. 107).

A Convenção Europeia para a Proteção dos Direitos Humanos, ratificada em 1950, e O Artigo 8 da Lei das Liberdades Fundamentais prevê a proteção de indivíduos sobre sua correspondência, sua vida privada e familiar, não podendo interferir exceto nos termos da lei e para proteger a democracia e a segurança 5 PAÍS (CONSEIL DE L'EUROPE; COUR EUROPÉENNE DES DROITS DE L'HOMME, 1950). Desde a segunda metade do século passado, os países europeus emendaram seu estatuto constitucional com disposições que reforçam a privacidade como direito fundamental, como no caso de Portugal, no seu artigo 65.º, ou mesmo na sequência esse movimento criou normas inconstitucionais de proteção de dados, como França, Alemanha e Dinamarca. Em 1981, a Comissão Europeia aprovou o principal marco vendo a questão do ponto de vista dos direitos fundamentais e dos marcos jurídicos transnacionais, a Convenção nº 108 (Parlamento Europeu, 1981).

A importância que a informação assumiu após a era industrial, especialmente na época posterior à década de 1980, fez com que o século XX fosse denominado como a era da

informação (SILVA FILHO, 2016). Em decorrência da importância da privacidade, foram criadas leis próximas do fim do século, e atualmente foram criadas leis e outras leis foram modificadas, com o objetivo de proteger a privacidade das pessoas e seus dados pessoais.

A Alemanha foi a precursora em legislação de privacidade e proteção de dados. Em 1970, o estado alemão de Hesse promulgou a primeira Lei de Proteção de Dados do mundo. Os outros estados seguiram logo em seguida e, em 1º de janeiro de 1978, a primeira Lei Federal de Proteção de Dados Alemã (BDSG) entrou em vigor. Esses atos estabeleceram princípios básicos de proteção de dados, como a exigência de uma permissão legal ou o consentimento do titular dos dados para qualquer tratamento de dados pessoais. Em 1983, o Tribunal Constitucional Federal Alemão considerou que o indivíduo tem o direito constitucional à autodeterminação informativa. O pano de fundo desse veredicto inovador foi um censo planejado para o ano de 1983, que se concentrou essencialmente no censo de toda a população alemã por meio de processamento eletrônico de dados. O povo alemão estava insatisfeito com esta ideia e como consequência mais de 1.600 queixas foram apresentadas no Tribunal Constitucional Federal contra a lei do censo que tinha sido especificamente adotada para o censo pelo parlamento alemão. Finalmente, em dezembro de 1983, o Tribunal Constitucional Federal Alemão declarou que certas disposições da Lei do Censo eram inconstitucionais. Esse veredito decidiu que os indivíduos seriam facilmente identificáveis pelos dados e reconheceu seu direito à “autodeterminação informativa”, como a constituição da Alemanha o chama. Esse veredicto estabeleceu o direito do indivíduo de permitir ou bloquear o compartilhamento de suas informações pessoais com qualquer entidade pública ou privada.

Em 1995 foi adotada na União Europeia a Diretiva 95/46/CE que regulamentou o tratamento de dados pessoais. A diretiva relativa à proteção de dados incidiu sobre a proteção dos indivíduos no que diz respeito ao tratamento e à livre circulação de dados pessoais, nos termos dela os dados pessoais só podiam ser transferidos para países fora da União Europeia se a organização fornecesse um nível adequado de proteção.

O Regulamento Geral sobre a Proteção de Dados (RGPD) 2016/679 é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais, o regulamento 2016/679

considera que ter direito sobre os próprios dados e garantia de proteção aos mesmos é um princípio fundamental na atual economia digital, pois "todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito" (União Europeia, 2016, p. 3). Foi aprovado em 15 de abril de 2016. Após um período de transição de dois anos, entrou em vigor em 25 de maio de 2018. Uma vez que o RGPD é um regulamento, e não uma diretiva, não é necessário que os estados-membros aprovem legislação adicional, pelo que o regulamento é vinculativo e aplicável, ou seja é um regulamento, logo permite que cada país tenha a sua própria lei de proteção de dados, desde que siga as diretrizes do regulamento. Isto permite alguma flexibilidade dentro de cada país, mas garante que os princípios basilares do mesmo são cumpridos por todos os Estados membros e pelas empresas que lidem nos referidos países ou que utilizem dados de cidadãos desses países.

O regulamento contempla todas as entidades que têm de cumprir as diretrizes. Isto é aplicável a todas as entidades que, de alguma forma, lidam com dados pessoais, à exceção do tratamento de dados efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas. Sejam estas empresas, institutos sociais, ou organismos públicos, desde que exista tratamento de dados pessoais, serão obrigadas a cumprir com o RGPD.

Na América Latina a Colômbia tem a mais desenvolvida legislação de proteção de dados com leis que estão sendo aplicadas desde 2012, porém o Chile foi o primeiro país a possuir uma lei de proteção de dados, em 1999, essa lei foi reformulada para se adequar a GDRP, outros países da América do Sul para se adequarem a GDPR criaram regulamentações como Argentina que a lei deles passou por discussões públicas e foi reformulada em 2018, O Brasil também está entre eles com a criação da LGPD.

Lei Carolina Dieckmann

Em 2012, a Lei Carolina Dieckmann foi aprovada para combater o cibercrime, na época, as redes sociais divulgaram uma notícia sobre o roubo de fotos íntimas da atriz brasileira

Carolina Dieckmann por meio da invasão de um e-mail. O criminoso exigiu o pagamento de certa quantia em dinheiro pela não publicação de fotos íntimas da atriz, por se tratar de figura pública e, portanto, de importância social, a Lei nº 12.737/2012, que alterou parte do Código Penal para caracterizar o uso ilícito de imagens, vídeos e outros dados pessoais sem consentimento, logo foi aprovada.

A Lei nº 12.737/2012 impactou o Direito Penal, pois acrescenta os artigos 154-A e 154-B ao Código Penal Brasileiro. Além disso, altera a redação dos artigos 266 e 298. A norma trata de uma tendência do Direito: segurança no ambiente virtual. Este projeto foi apresentado em 29/11/2011 e aprovado pela Presidente Dilma Rousseff em 02/12/2012. Foi o primeiro texto a descrever crimes cibernéticos e focado em dispositivos que ocorrem sem a permissão do proprietário. Vale lembrar que as leis demoram anos para serem aprovadas no Brasil, mas, nesse caso, foi sancionada por pressão da mídia após um incidente com uma personalidade famosa, então demorou um tempo recorde, apenas um ano.

O primeiro Artigo 15 introduziu o delito denominado "intrusão de computador" que consiste na invasão de qualquer outro computador, como computadores, smartphones, tablets etc. conectados à Internet ou não, o ato deve ser realizado quebrando o mecanismo de segurança e sua finalidade é corromper, obter ou destruir dados sem a permissão do proprietário do dispositivo, a norma também vale para quem instala brechas de segurança (como vírus) em aparelhos para obter benefícios ilícitos.

Quem produz, oferece, distribui, vende ou distribui programa ou aparelho de computador que possibilite o exercício, também sofre as consequências do crime, este crime é processado por representação, ou seja, o Ministério de Estado só apresenta queixa se a vítima o solicitar, salvo se o crime for cometido (direta ou indiretamente) contra a administração pública, ou seja, governo municipal, estadual ou federal, bem como empresas prestadoras de serviço público.

A pena para o crime de dispositivos hackeados é de 3 meses a 1 ano de prisão mais multa, mas a pena é aumentada em 1/6 se causar prejuízo financeiro à vítima, se o crime envolver a aquisição de conteúdo de comunicações privadas, segredos comerciais ou de trabalho, telecomando de equipamentos ou informação confidencial, a pena é de prisão de 6

meses a 2 anos, mais multa - salvo se o facto constituir crime mais grave . Neste último caso, a multa é aumentada de 2/3 se as informações recebidas forem transmitidas, distribuídas ou vendidas.

Por fim, a pena pode ser aumentada de 1/3 à metade, se o crime for dirigido contra as seguintes autoridades: prefeito, governador ou presidente da república; Presidente do Supremo Tribunal Federal (STF); Presidentes de governos locais, parlamentos estaduais ou sindicais, como Senado Federal, Câmara Municipal, Câmara Legislativa etc., altos dirigentes do governo municipal, estadual ou federal.

O texto ainda acrescenta os parágrafos 1º e 2º no artigo 266, fazendo com que incorra com as mesmas consequências do artigo quem interrompe, impede ou dificulta serviços de informação que sejam públicos. Ademais, a pena é dobrada quando o ato é cometido em calamidades públicas (situação anormal como desastres naturais), a alteração do artigo 298 consiste na adição de um parágrafo único que equipara os cartões de crédito ou débito como documentos particulares, na hipótese que ocorrerem crimes de falsificação de documento.

Escândalo Cambridge Analytica

A *Cambridge Analytica* é uma empresa de análise de dados que trabalhou com o time responsável pela campanha do republicano Donald Trump nas eleições de 2016, nos Estados Unidos. A empresa teria comprado acesso a informações pessoais de usuários do Facebook e usado esses dados para criar um sistema que permitisse predizer e influenciar as escolhas dos eleitores nas urnas, segundo a investigação dos jornais *The Guardian* e *The New York Times*.

As informações dos usuários do Meta foram coletadas por meio de um teste psicológico chamado de "*This is your digital life*", utilizou uma brecha nos termos e condições do Facebook que não proibia expressamente a venda de dados coletados na rede social por aplicativos, pagou

a centenas de milhares de usuários pequenas quantias para que eles fizessem um teste de personalidade e concordassem em ter seus dados coletados para uso acadêmico.

O aplicativo foi desenvolvido por *Aleksandr Kogan*, pesquisador da Universidade de Cambridge, no Reino Unido. Ele tinha uma pesquisa sobre como deduzir a personalidade e as inclinações políticas das pessoas a partir de seus perfis no Facebook. A *Cambridge Analytica* que não tem relação nenhuma com a Universidade de Cambridge comprou os dados coletados por ele.

A *Cambridge Analytica* se declarou culpada no dia 09/01/2019 por descumprir uma ordem do regulador britânico encarregado da proteção de dados (ICO, na sigla em inglês), que mandou que ela revelasse as informações que tinha sobre um professor americano, David Carroll. Carroll havia pedido para saber quais dados sobre ele a companhia tinha e como os havia obtido.

O escândalo *Cambridge Analytica*, como ficou conhecido, chamou a atenção e indignação da mídia, do público, de parlamentares e reguladores em todo o mundo - demonstrando que sim, as pessoas se preocupam com violações de sua privacidade e abuso de poder. Este escândalo foi um dos muitos que ilustram que a privacidade também diz respeito à autonomia, dignidade e autodeterminação das pessoas - e uma pré-condição necessária para a democracia. Ao mesmo tempo, o GDPR, que levou anos para ser criado, finalmente entrou em vigor em toda a UE em 25 de maio de 2018, trazendo consigo obrigações rigorosas para quem usa dados pessoais e direitos mais fortes para os indivíduos, tanto dentro como fora da UE.

Lei de Proteção de Dados- LGPD

No Brasil, a LGPD é um importante marco legislativo brasileiro que altera claramente o atual padrão de coleta e processamento indiscriminado de dados pessoais processe apenas o necessário para o modelo em que será coletado. LGPD contribui para que fundações que enfatizam a proteção dos direitos e garantias das pessoas físicas, como exemplos incluem respeito à privacidade, autodeterminação de informações, liberdade de expressão, Inviolabilidade da Privacidade, Desenvolvimento Econômico e Tecnológico Além da Liberdade Defesa e respeito aos direitos humanos.

A referida legislação regula apenas o tratamento de dados pessoais, Garantir o direito fundamental à liberdade, e privacidade dos cidadãos, pois "rege o tratamento de dados pessoais, inclusive em meio digital, [...] proteger os direitos fundamentais de liberdade e privacidade e livre desenvolvimento da personalidade das pessoas físicas" (BRASIL, 2019 d), ao invés de incluindo dados de entidades legais, informações confidenciais, patentes ou software, títulos descritivos, pois tais informações estão protegidas pelo Diploma de Direito os sistemas jurídicos nacionais existentes, como a Lei da Propriedade Industrial (Lei 9.279/1996), Lei de Software (Lei 9.609/1998) e Lei de Propriedade Industrial (Lei 9.609/1998) 9.610/1998).

A LGPD passou por um longo processo de criação no Congresso Nacional e também por grande debate entre os mais diversos setores da sociedade, esse debate teve como objetivo assegurar aos usuários o direito de saber como será realizado o consentimento, uso e tratamento de seus dados, foi criada utilizando como base a General Data Protection Regulation(GDPR), lei de proteção de dados europeia com o objetivo de proteger os dados pessoais (informações relacionadas apenas às pessoas físicas), a liberdade e a privacidade das pessoas que submetem ou tem seus dados coletados por terceiros, garantindo, assim, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico e tecnológico e a inovação.

A LGPD possui obrigações tanto para o setor público quanto o privado, são elas obter o consentimento do titular de dados, realizar o tratamento de dados, No ato da obtenção do consentimento a empresa precisará disponibilizar um contato ao titular (inclusive com identificação do Encarregado de Tratamento de Dados - *Data Protection Officer* - DPO) preferencialmente no site da empresa, bem como especificar que seus colaboradores e pessoas que terão acesso aos dados obtidos estão sob responsabilidade (e treinamento), se os dados forem obtidos como condição necessária para o fornecimento de um produto ou serviço o titular dos dados deverá ser informado sobre este fato, de forma destacada.

Os dados pessoais são um recurso importante para atividades comerciais, sociais e pessoais, bem como para a implementação de políticas públicas e desenvolvimento econômico global, e a LGPD define dados pessoais como informações relacionadas a uma pessoa natural identificada ou identificável, conforme o artigo 5º, parágrafo 3º. I (BRASIL, 2019d). Portanto, pode ser considerada uma informação que, individualmente ou em conjunto, permite a identificação de uma pessoa singular, tais como brasão, nome, nome próprio, estado civil, Número de contribuinte, bilhete de identidade, estado civil, profissão, dados relativos à origem

social ou étnica, saúde, convicções políticas ou religiosas, são exemplos de dados pessoais que permitem a extração. de informação geral que não tem relação objetiva com uma pessoa (DONEDA, 2006, p. 157). Portanto, fica claro que a LGPD visa proteger as violações daqueles recursos ou características, que constituem uma projeção da pessoa humana (BITTAR, 2015, p. 1).

Os dados pessoais considerados sensíveis enquadram-se numa categoria especial. (LGPD Art. 5º inciso II) pois podem sujeitar os dados a práticas discriminatórias. Dados sensíveis são, por exemplo, dados sobre origem étnica, crenças religião, opiniões políticas, filiação sindical, saúde, vida sexual, dados genéticos, dados biometria etc. A base legal para o tratamento destes dados deve ser mais cumprida restritivas em comparação com os dados pessoais, as preocupações dos legisladores se relacionam com provavelmente riscos e vulnerabilidades mais graves aos direitos fundamentais (VAINZOF, 2019, p. 92).

A empresa precisará, no ato do consentimento, especificar todos os direitos do titular dos dados, em caso de compartilhamento dos dados coletados com terceiros é necessária a obtenção de consentimento específico para o referido fim, não utilizar posteriormente os dados coletados para fins que não sejam os que foram previamente informados ao titular, o qual aceitou os termos na ocasião da coleta, limitar o tratamento utilizando o mínimo de dados possíveis, proporcionar livre acesso, inclusive gratuito e facilitado, aos dados coletados exclusivamente aos respectivos titulares, inclusive com a possibilidade de revogação do consentimento concedido. Implementar sistemas de segurança aptos a proteger os dados coletados contra terceiros não autorizados, adotar medidas para garantir a transparência do tratamento de dados e prevenir a ocorrência de danos em virtude do tratamento dos dados. Não utilizar os dados coletados para fins ilícitos ou abusivos. Demonstrar a adoção de todas estas medidas e comprovar a eficácia das mesmas, como por exemplo, expor de forma detalhada a gestão dos dados em política de privacidade do site, manter registro das operações de tratamento de dados pessoais que realizar.

A LGPD possui sete fundamentos que são o respeito à privacidade; à autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

O conceito de tratamento do artigo 5º, inciso X, é fundamental para o entendimento da LGPD. De fato, a legislação é abrangente quanto à definição de tratamento, porque considera todo o ciclo de vida dos dados, desde a coleta até a exclusão, incluindo as mais diversas operações de tratamento. A conformidade deste escopo está na letra da lei, significando todas as atividades como, além do acima, produção, recebimento, classificação, uso, acesso, armazenamento, exclusão, modificação, comunicação, transferência, para citar apenas um alguns exemplo (BRASÍLIA, 2019 d). segue os princípios listados.

O Artigo 5 da LGPD apresenta definições de termos que são utilizados na lei, essas definições são:

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

Dado pessoal 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;

Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

Relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

Órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico;

Autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

No artigo 6º da LGPD, há princípios gerais, como as normas básicas , que são consideradas decisivas e constituem a espinha dorsal das normas de proteção de dados atualmente em vigor, como transparência, finalidade, adequação, necessidade, proporcionalidade, qualidade e acesso livre. , considerando que "o tratamento de dados pessoais deve observar os princípios de boa fé e finalidade; suficiência; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; responsabilidade" (BRASILIO, 2019d) Portanto, além do fato de que o processador responsável controla a possibilidade de tratamento e cumpre uma base legal, preste atenção ao cumprimento dos princípios listados.

Para que o tratamento de dados pessoais ocorra de forma legal e lícita, é necessário revisar e cumprir rigorosamente as bases legais estabelecidas na legislação . A base legal é a hipótese, que permite o tratamento de dados pessoais, e é importante que o programa de adaptação realize um mapeamento dos dados pessoais para avaliar o enquadramento do tratamento em uma das bases legais existentes durante todo o ciclo de vida dos dados [...]. Caso não encontrem uma das bases legais, deverá suprir essa lacuna" (VAIZONF, 2019, p. 116). Entre as bases legais, podemos citar o consentimento dado pelo proprietário do; cumprimento de obrigações legais; implementação da ordem pública; realização de pesquisas por uma instituição de pesquisa; execução de um contrato do qual o proprietário é parte; exercício regular de direitos em juízo judicial, administrativo ou arbitral proteção de vidas, proteção da saúde, atendimento aos interesses legítimos do responsável pelo tratamento e por fim proteção do crédito.

O artigo 18 da LGPD lista direitos específicos que podem ser exercidos por qualquer pessoa física titular de dados pessoais, ressalvadas as hipóteses previstas em lei. O controlador de dados (responsável pelas decisões sobre o tratamento de dados pessoais) deve receber todas as solicitações de dados de alguma forma e não pode ignorá-las (MALDONADO, 2019, p. 221). Destacam-se os seguintes direitos dos proprietários: acesso aos dados, ou seja, o direito de saber sobre o processamento e a existência de dados pessoais; correção de dados incorretos; exclusão de dados se eles forem desnecessários ou processados incorretamente após a retirada do consentimento; e retirada de consentimento (BRASIL, 2019 d).

A LGPD define as regras sobre padrões de segurança da informação e medidas administrativas para a proteção de dados pessoais que os controladores e operadores (aqueles que processam dados pessoais em nome do controlador) devem seguir. Ou seja, os recursos

técnicos – aprovados no âmbito da tecnologia da informação e governança – como parte da política empresarial, gestão estratégica e capacitação (BRUNO, 2019, p. 330) devem ser adequados à LGPD.

A LGPD possui duas ferramentas para assegurar a privacidade dos dados e ajudar as empresas cumprirem a lei de proteção dados, essas ferramentas são o RIPD e o IDP, o RIPD é um relatório onde é relatado os possíveis riscos à privacidade do Titular, também deve apresentar todas medidas e mecanismos de mitigação de riscos adotados pelo controlador no processo de tratamento de dados, e é um documento pedido peça ANPD. O IDP auxilia na criação do RIPD pois mapeará todo o funcionamento do tratamento de dados, esse documento ajudará a empresa cumprir algumas obrigações com a LGPD. Como disponibilizar um contato ao titular (inclusive com identificação do Encarregado de Tratamento de Dados- *Data Protection Officer* - DPO) preferencialmente no site da empresa, bem como especificar que seus colaboradores e pessoas que terão acesso aos dados obtidos estão sob responsabilidade.

FERRAMENTAS UTILIZADAS NO DESENVOLVIMENTO DA APLICAÇÃO E SISTEMAS CORRELATOS

A *Privacy Tools* é uma plataforma de gerenciamento da privacidade com módulos pensados para o uso em diferentes segmentos do mercado e para cumprir com as obrigações das diferentes legislações, como LGPD e GDPR.

A *LGPDY* é uma plataforma que oferece soluções para controle sobre a política de *cookies* e rastreadores utilizados na maioria dos *sites*. A proposta é ser transparente com os usuários através do consentimento de uso de cookies. Para que seja feito o consentimento, a plataforma permite criar o *plugin* customizado de notificação que aparece sempre que um usuário acessa o site, assim é feita a comunicação sobre o uso de cookies e solicitado o

consentimento. Caso o usuário opte por não utilizar os cookies, a *LGPDY* faz o bloqueio automático dos *cookies* do *site* até que o usuário dê o consentimento.

FERRAMENTAS E TECNOLOGIA

HTML 5

As páginas da web são estruturadas através do *Hypertext Markup Language* (Linguagem de Marcação de Hypertexto). A criação da página ocorre através de *tags* que informam ao navegador como ele deve apresentar o conteúdo, através das quais é informado se aquela estrutura é um *tag* ou uma tabela *tag table*. O número de etiquetas é grande, existindo cerca de 116 representações de estruturas na versão 5.

CSS

Css é chamado de linguagem *Cascading Style Sheet* e é usado para estilizar elementos escritos em uma linguagem de marcação como HTML. O CSS separa o conteúdo da representação visual do site, ou seja, css define o estilo e descreve como o html deve ser exibido.

A especificação do CSS é desenvolvida pela W3C e pode ser encontrada na página oficial da especificação no site W3C. Atualmente ele está em sua terceira versão.

JavaScript

É uma linguagem leve, interpretada e baseada em objetos com funções de primeira classe, mais conhecida como a linguagem de *script* para páginas *Web*, mas usada também em vários outros ambientes sem *browser*, tais como node.js, Apache *CouchDB* e Adobe Acrobat. O JavaScript é uma linguagem baseada em protótipos, multi-paradigma e dinâmica, suportando estilos de orientação a objetos, imperativos e declarativos (como por exemplo a programação funcional). Saiba mais sobre o JavaScript.

Foi utilizada no *front-end* do projeto para gerar um pdf ou imprimir os relatórios salvo no banco de dados o *onclick="window.print()* permitir isso, e outra quando o encarregado estiver cadastrando as senhas serão comparadas, e só vai permitir salvar se as duas forem iguais

Código para comparar as senhas

```
<script>
     let senha = document.getElementById('senha');
    let senhaC = document.getElementById('senhaC');

    function validarSenha() {
      if (senha.value != senhaC.value) {
        senhaC.setCustomValidity("Senhas diferentes!");
        senhaC.reportValidity();
        return false;
      } else {
        senhaC.setCustomValidity("");
        return true;
      }
    }

    // verificar também quando o campo for modificado,
    senhaC.addEventListener('input', validarSenha);

</script>
```

fonte: autor

Bootstrap

Bootstrap é um *framework front-end* que fornece estruturas de CSS para a criação de *sites* e aplicações *responsivas* de forma rápida e simples. Além disso, pode lidar com sites de *desktop* e páginas de dispositivos móveis da mesma forma é de código-fonte aberto para desenvolvimento de componentes de interface e *front-end para sites* e aplicações web, usando HTML, CSS e JavaScript, baseado em modelos de design para a tipografia, melhorando a experiência do usuário em um site amigável e responsivo.

Originalmente, o Bootstrap foi desenvolvido para o *Twitter* por um grupo de desenvolvedores liderados por Mark Otto e Jacob Thornton Logo e se tornou uma das estruturas de *front-end* e projetos de código aberto mais populares do mundo. Antes de ser uma estrutura de código-fonte aberto, o Bootstrap era conhecido como *Twitter Blueprint*. Após alguns meses de desenvolvimento, o Twitter realizou sua primeira Hack Week: o projeto ganhou uma grande popularidade quando desenvolvedores de todos os níveis de habilidade usaram o framework sem qualquer orientação externa. Após o evento, ele serviu como guia de estilo para o desenvolvimento de ferramentas internas na empresa por mais de um ano antes de seu lançamento se tornar público.

Thymeleaf

É um mecanismo de modelo Java moderno do lado do servidor para ambientes da Web e independentes, traz modelos naturais elegantes para o seu fluxo de trabalho de desenvolvimento - HTML que pode ser exibido corretamente em navegadores e também funcionar como protótipos estáticos, é ideal para o desenvolvimento da web HTML5 JVM moderno - embora haja muito mais que ele pode fazer.

Java

O Java foi criado em 1995 na empresa Sun Microsystem por uma equipe liderada por James Gosling, o Java foi adquirido pela empresa Oracle em 2008.

O Java é uma linguagem de programação orientada a objetos e mesmo com mais 25 anos continua sendo extremamente utilizada no desenvolvimento de aplicações WEB, Mobile e Desktop.

Algumas características do Java: O código de um programa escrito em Java é compilado para uma forma de *bytecode*, que é interpretada pela JVM; A necessário ter conhecimento sólidos dos conceitos de orientação a objeto para o uso da linguagem, tendo em vista que tudo desenvolvido dentro da linguagem Java utilizar classes e objetos; Java é uma linguagem de Tipagem Estática; JDK O kit de desenvolvimento Java é um conjunto de utilitários que permite criar sistemas de software para a plataforma Java.

Padrão Objeto de Transferência de Dados- DTO é um padrão de projeto que foi utilizado no projeto, esse padrão é usado e para o transporte de dados entre diferentes componentes de um sistema, diferentes instâncias ou processos de um sistema distribuído ou diferentes sistemas via serialização, evitar expor todos os dados da nossa camada de persistência.

MVC é uma arquitetura de software que divide seu aplicativo em três camadas. Camada de interação com o usuário (*View*), camada de processamento de dados (model) e camada de controle (*Controller*). A *view* só mostra os dados (html/xml), o model é responsável pela leitura e escrita dos dados (exceto para validação). E o *Controller* é o responsável por receber todas as requisições do usuário e seus métodos chamados de ações são os responsáveis pela página controlar qual *template* é utilizado e qual *view* é mostrado ao usuário. A ordem de criação das classes e pacotes do projeto é: Modelo (entidade), Repositório, Serviço, Controlador. O pacote de modelos são onde residem os modelos de aplicativo. O pacote *Repository* é o local onde se encontra a classe que faz transações com o banco de dados, ou seja, é o modelo de desenho em

que os dados são obtidos do banco de dados e também ocorre a regra de negócio. Ele retorna objetos de domínio que seriam entidades (classes anotadas com @Entity). Esta é a subcamada responsável pela persistência dos dados (*fetch, update, insert, delete*). · Serviço é outro padrão de projeto que possui apenas uma regra de negócios e nenhum acesso direto ao banco de dados. É a subcamada responsável pela regra de negócio (válida os dados, executa a regra de negócio, utiliza a *data store* e a entidade para acessar os dados e armazenar os dados). · Um *controller* é usado para conectar uma *view* a outras partes do sistema, que são a regra de negócio e o banco de dados.

Spring Boot

Spring boot foi criado em abril de 2014, o seu objetivo é facilitar o trabalho de configuração e proporcionar ao desenvolvedor que sua aplicação seja publicada o mais rápido possível.

O Spring boot foi baseado no conceito convenção sobre configuração, o spring boot configura tudo utilizando servidor *tomcat* embarcado. Mas há a possibilidade de customizar o que for necessário posteriormente. Alguns dos módulos utilizados na configuração do *spring* boot são *WEB, DevTools, Spring Batch, Spring Data JPA*, entre muitos outros. O objetivo do Spring Boot é facilitar o processo das configurações iniciais das aplicações WEB em Java. Consequentemente, ele traz mais agilidade para o processo de desenvolvimento, uma vez que os desenvolvedores conseguem reduzir o tempo gasto com as configurações iniciais.

Interface EncarregadodeDadosService

```java
package com.example.geradorDeRelatoriosLgpd.service;

import org.springframework.security.core.userdetails.UserDetailsService;



public interface EncarregadoDeDadosService extends UserDetailsService {
    EncarregadoDeDados save(EncarregadoDeDadosRegistrationDto registrationDto);
}
```

fonte:Autor

Foi implementado a interface UsuárioDetalhesServiço na interface EncarregadoService, a UsuárioDetalhesServiço carrega dados específicos do usuário. Ele é usado em toda a estrutura como um DAO do usuário e é a estratégia usada pelo DaoAuthenticationProvider. A interface requer apenas um método somente leitura, o que simplifica o suporte para novas estratégias de acesso a dados, a interface EncarregadoService foi implementada na classe EncarregadoDeDadosServiceServiceImpl para poder utilizar o método loadUserByUsername que vai permitir logar.Metodo loadUserbyname que vai permitir logar.

Metodo loadUserbyname

```
@Override
public UserDetails loadUserByUsername(String username) throws UsernameNotFoundException {
    System.out.println("email" + username);
    EncarregadoDeDados encarregadoDeDados = encarregadoDeDadosRepository.findByEmail(username);

    if(encarregadoDeDados == null) {
        throw new UsernameNotFoundException("Invalid username or password.");
    }
    return new org.springframework.security.core.userdetails.User(encarregadoDeDados.getEmail(),
            encarregadoDeDados.getSenha(), mapRolesToAuthorities(encarregadoDeDados.getRoles()));
}

private Collection<? extends GrantedAuthority> mapRolesToAuthorities(Collection<Role> roles){
    return roles.stream().map(role -> new SimpleGrantedAuthority(
            role.getName())).collect(Collectors.toList());
}
```

fonte: Autor

Spring Security é uma estrutura de autenticação e controle de acesso poderosa e altamente personalizável. É o padrão de fato para proteger aplicativos baseados em Spring.

Spring Security é uma estrutura que se concentra em fornecer autenticação e autorização para aplicativos Java. Como todos os projetos do Spring, o verdadeiro poder do Spring Security é encontrado na facilidade com que pode ser estendido para atender aos requisitos personalizados.

O *Método Save* foi onde eu passei os dados do *dto* para salvar eles e criptografar a senha, método *encode()* que passawordEncode traz, serve para converter a senha simples na forma codificada.

Método save

```
@Override
public EncarregadoDeDados save(EncarregadoDeDadosRegistrationDto registrationDto) {
    if (emailExists (registrationDto.getEmail())) {
        throw new UserAlreadyExistException("There is an account with that email address: "
          + registrationDto.getEmail());
    }
    EncarregadoDeDados encarregadoDeDados =
            new EncarregadoDeDados( registrationDto.getNome()
                    ,registrationDto.getEmail(),registrationDto.getTelefone(),registrationDto.getEmpresa(),
            registrationDto.getCep(),registrationDto.getCidade(),
            registrationDto.getEndereco(), passwordEncoder.encode(registrationDto.getSenha())
            ,Arrays.asList(new Role("ROLE_USUARIO")));

    return encarregadoDeDadosRepository.save(encarregadoDeDados);

}
```

fonte: Autor

A classe *SecurityConfigure* classe base e substituindo métodos individuai foi adicionada anotação a uma @Configurationclasse para ter a configuração do *Spring Security* definida em qualquer *WebSecurityConfigurer* ou mais provavelmente estendendo a *WebSecurityConfigurerAdapterclass*, A *@EnableWebSecurityé* uma anotação de marcador. Ele permite que o Spring encontre (é um *@Configuratione*, portanto, *@Component*) e aplique automaticamente a classe ao *WebSecurity*.

O método *configure* em que é determinado quais páginas o usuário que no caso do meu sistema é o encarregado, vai ter acesso sem senha e quais ou qual conjunto de páginas que ele precisa logar para acessar.

Classe SecurityConfigure

```
@Configuration
@EnableWebSecurity
public class SecurityConfiguration extends WebSecurityConfigurerAdapter {
    @Autowired

    private EncarregadoDeDadosServiceServiceImpl encarregadoDeDadosservice;

    @Bean
    public BCryptPasswordEncoder passwordEncoder() {
        return new BCryptPasswordEncoder();
    }

    @Bean
    public DaoAuthenticationProvider authenticationProvider() {
        DaoAuthenticationProvider auth = new DaoAuthenticationProvider();
        auth.setUserDetailsService(encarregadoDeDadosservice);
        auth.setPasswordEncoder(passwordEncoder());
        return auth;
    }
```

fonte: Autor

método Configure

```
@Override
protected void configure(HttpSecurity http) throws Exception {
    http.authorizeRequests().antMatchers(
                    "/register**").permitAll()
            .anyRequest().authenticated()
            .and()
            .formLogin()
            .loginPage("/login")

            .permitAll()
            .and()
            .logout()
            .invalidateHttpSession(true)
            .clearAuthentication(true)
            .logoutRequestMatcher(new AntPathRequestMatcher("/logout"))
            .logoutSuccessUrl("/login?logout")

            .permitAll();
}
```

fonte: Autor

Hibernate

Trabalhar com software orientado a objetos e bancos de dados relacionais pode ser complicado e demorado. Os custos de desenvolvimento são significativamente mais altos devido a uma série de "incompatibilidades de paradigma" entre como os dados são representados em objetos e em bancos de dados relacionais. O *Hibernate* é uma solução de Mapeamento Objeto/Relacional (ORM) para ambientes Java. O termo Mapeamento Objeto/Relacional se refere à técnica de mapeamento de dados entre uma representação de modelo de objeto e uma representação de modelo de dados relacional.

Segundo a documentação de referência do *Hibernate* (2011). “O *Hibernate* é um *framework* que implementa a API de referência e até outros métodos próprios de seu *framework*”, além de ser o mais utilizado do mercado de software para mapeamento objeto/ relacional. Segundo a documentação de referência do *Hibernate* (2011). “Dando suporte total a API JPA 2.0.”

“O termo mapeamento objeto / relacional refere-se à técnica de mapeamento de dados a partir de uma representação do modelo de objeto em uma representação de dados relacionais do modelo e vice-versa.” (Hibernate em Ação 2008) “O Objetivo do JPA é abstrair do desenvolvedor a maioria das tarefas comuns de programação relacionadas com a persistência, eliminando, muitas vezes, a necessidade manual de processamento de dados feito à mão usando SQL e JDBC.” (JPA com Hibernate 2007).

As principais notações utilizadas no projetam foram: a anotação @Autowired executa a injeção de dependência (para que as instâncias do repositório possam ser usadas), anotação da classe @Service indica que é um bean gerenciado Spring MVC (é um serviço), @Controller indica que a classe do controlador é um bean de primavera e a anotação @RequestMapping especifica qual método HTTP usar e qual é sua URL. Por exemplo, em @RequestMapping (valor = "/posts", método = RequestMethod.GET), temos a URL "/posts" e o método HTTP é GET (pega os dados do banco de dados e retorna).

Pelo RIPD e o Inventário são formulários com diversos campos, com algumas perguntas a serem respondidas se repetiam, então os atributos que se repetiam foram declarados como um *ArryList de String,* foi necessário Utilizar as notações *@ElementCollection e o OrderCollection,* pois sem eles o *hibernate* não iria mapear esse tipo de dados, e aconteceria o erro *Multiple Bags*, o *Hibernate* não reconhece o tipo *list*, poderia evitar o erro utilizando o tipo *set* porém ele não aceita repetição e não seria bom para esse caso, a notação *@Column* foi necessária pois alguns dados passados eram muito grande e ocorria o truncamento de dados em algumas parte da tabelas do banco.

Atributos

```
private String finalidade;
@Column(columnDefinition="LONGTEXT")
private String pInteressada;

@Column(columnDefinition="LONGTEXT")
private String ncProporcionalidade;

@OrderColumn(name = "position")
@ElementCollection(fetch = FetchType.EAGER )
@Column(columnDefinition="LONGTEXT")
private List<String> risco = new ArrayList<String>();
```

fonte: autor

MySQL

MySQL é um sistema de gerenciamento de banco de dados relacional SQL de código aberto desenvolvido e com suporte da Oracle. O MySQL foi originalmente lançado em 1995. Desde então, ele passou por algumas mudanças de proprietário e administração antes de ser comprado pela Oracle Corporation em 2010. Embora a Oracle esteja no comando agora, o MySQL ainda é um *software* de código aberto, o que significa que você pode usá-lo e modificá-lo livremente.

Para exibir os dados foi necessário para grande deles passar a posição do vetor, para que os dados fossem mostrados separados e na posição certa.

Exibição dos dados

```
        </td>

        <td>
            <a><span th:text="${ripd.riscoTratamento[0]}"></span></a>
        </td>
        <td>
            <a><span th:text="${ripd.p1[0]}"></span></a>
        </td>
        <td>
            <a><span th:text="${ripd.i1[0]}"></span></a>
        </td>
        <td>
            <a><span th:text="${ripd.nivelRisco[0]}"></span></a>
        </td>

    </tr>
```

Fonte Autor

DESENVOLVIMENTO DA APLICAÇÃO

Para o desenvolvimento da aplicação é fundamental saber quais são as necessidades a respeito do Inventário de Dados e do Relatório de Impacto à Proteção Dados Pessoais, em razão de que o escopo deste trabalho é exatamente o desenvolvimento de uma aplicação web para apoiar as atividades relacionadas a essas questões.

Inventário de Dados

O inventário de dados refere-se a um documento essencial quando estamos no processo de adequação às normas de proteção de dados, no caso do Brasil a LGPD, é um documento ou

uma planilha que deve mostrar o caminho que o dado pessoal da empresa e procedimentos, processos pelo qual o dado percorre. O documento apresenta um panorama geral de como a empresa está lidando com a questão da privacidade e segurança da informação.

É um documento essencial quando estamos no processo de adequação às normas de proteção de dados (LGPD, GDPR, CCPA), que deve ser elaborado em conjunto pelos múltiplos setores das empresas com auxílio técnico e jurídico para análises das possíveis vulnerabilidades encontradas.

Os principais objetivos do Inventário de Dados Pessoais (IDP) é identificar a forma como a empresa lida com a privacidade e a segurança da informação de seus clientes, colaboradores e parceiros terceirizados, cumprindo, desta forma, a exigência constante no art. 37 da LGPD em que estipula que o controlador, que é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, e o operador que é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, devem manter registro das operações de tratamento de dados pessoais.

A seguir, será mostrado pontos essenciais que devem estar contidos no inventário de dados.

Quadro 1- Informações necessária do Inventário de Dados

Tema	**Itens**
Tipos de dados	Categorias de dados trafegadas nesse fluxo (ex: cadastrais, transacionais, especiais, sensíveis, trabalhistas etc.)
Etapas do fluxo de dados	Descrição das etapas de tratamento do fluxo: coleta, armazenagem, sanitização, enriquecimento, processamento, segmentação, inferências, transferências,

Locais de Armazenamento	Indicar os locais onde o dado é coletado, armazenado, tratado ou processado. Nesse momento, deve-se indicar se é internamente ou externamente.
Tecnologias	Apontar no mapeamento de dados as principais tecnologias utilizadas nesse fluxo de dados. (ex: sistemas, aplicações, bancos de dados que suportam o fluxo, etc.)
Origem dos Dados	Indicar as principais origens dos dados (entradas) e canais de captura de dados (ex: site, aplicativos, estabelecimentos físicos, SAC, parceiros, empresas coligadas, etc.)
Campanhas de Marketing	Informar como os dados pessoais são tratados visando campanhas de marketing. Indicar também no mapeamento de dados quais os tipos de dados pessoais são utilizados
Compartilhamento de dados com parceiros	Indicar os principais parceiros com os quais os dados são compartilhados – parceiros de negócio ou parceiros de tecnologia/dados (ex: *slack*, escritório de contabilidade terceirizado, emissor de NFe, etc.)
Empresas coligadas	Indicar no mapeamento de dados as empresas coligadas do grupo econômico cujos dados são compartilhados entre si.
Localidades do tratamento	Indicar os países, estados e localidade onde sua empresa possui atividade.
Base legal	Indicar a base legal para realização do tratamento de dados referente ao fluxo descrito.
Transferência Internacional de dados	• Plataformas de *cloud* (ex: *amazon aws, microsoft azure, google cloud);* • *Data centers* terceirizados; • *Software* terceirizados; Transferência de dados pessoais para a sede da empresa no exterior.

Política de Privacidade	A Política de privacidade referente ao fluxo descrito está atualizada e atende aos requisitos da LGPD? Ela está disponível em todas as fases da coleta de dados?
Dados de menores de idade	Identificar se no fluxo analisado há a coleta de dados pessoais de menores de idade (18 anos incompletos). Verificar se todos os registros possuem data de nascimento informada é válida.
Segurança da Informação	Identificar os principais controles de segurança da informação estabelecidos para proteger os dados coletados, armazenados, processados, compartilhados e transferidos.
Retenção e extinção de dados	Identificar a política de retenção e extinção (descarte) dos dados. Caso não exista, avaliar as boas práticas do setor da empresa e por categoria de dados.
Direito dos Titulares	Avaliar se o fluxo permite que o titular do dado pessoal tratado exerça seus direitos previstos nas normas de proteção de dados.

Fonte: lb consultoria digital(2020)

Relatório de Impacto à Proteção de Dados (RIPD)

O RIPD é a sigla para Relatório de Impacto à Proteção de Dados, uma das exigências previstas na LGPD. Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

O Relatório de Impacto à Proteção de Dados (RIPD) é focado nos direitos dos indivíduos, de forma que: 1) o conceito do relatório de impacto prevê a elaboração desse instrumento quando as atividades puderem gerar "riscos às liberdades civis e aos direitos fundamentais" (artigo 5º, XVII, LGPD); e 2) entre as competências da Autoridade Nacional de

Proteção de Dados (ANPD) está regulamentar o RIPD para os casos em que o tratamento representa "alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na lei" (artigo 55-J, XIII, LGPD).

O Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) é um documento que o controlador tem a responsabilidade da elaboração, cumpre a função de demonstrar como os dados pessoais são coletados, tratados, usados, compartilhados e quais medidas são adotadas para diminuição dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados, ou seja constitui uma ferramenta de gestão de riscos à privacidade.

Figura 1- Etapas do RIPD

Fonte: governo digital (2020)

A etapa 1 consiste em identificar os agentes de tratamento (controlador e operador) e o encarregado no RIPD. Nesta primeira etapa, basta identificar os três envolvidos. No caso do Data Protection Officer(DPO) conhecido como Encarregado de Dados, é preciso incluir o nome, e-mail e telefone.

A etapa 2, segundo diretriz desenvolvida pelo Article 29 *Working Party* (WP29)*, os critérios relevantes de avaliação das operações suscetíveis à um RIPD são: Avaliação, classificação ou *scoring*, incluindo definição de perfis e previsão de aspectos relacionados com o desempenho profissional, a situação econômica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou movimento do titular; decisões automatizadas que produzam efeitos jurídicos ou efeito similar; monitoramento sistemático; dados sensíveis ou de natureza altamente pessoal; tratamento de dados em larga escala; combinação de conjuntos de dados; dados de titulares vulneráveis; uso inovador ou aplicação de novas soluções tecnológicas ou organizacionais, quando o tratamento dos dados visa permitir ou negar o acesso do titular a determinado serviço ou realização de um contrato.

Na etapa 3, é preciso também descrever os processos de tratamento de dados pessoais que possam gerar riscos, especificando a natureza, o escopo, o contexto e a finalidade do tratamento. A natureza do tratamento mostra como a organização trata ou pretende tratar o dado pessoal.

Na etapa 4, é importante destacar todas as partes consultadas sobre o tratamento abrangido pelo relatório, partes interessadas relevantes, internas e externas, consultadas a fim de obter opiniões legais, técnicas ou administrativas sobre os dados pessoais que são objeto do tratamento.

Na etapa 5, demonstrar que as operações realizadas sobre os dados pessoais limitam o tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

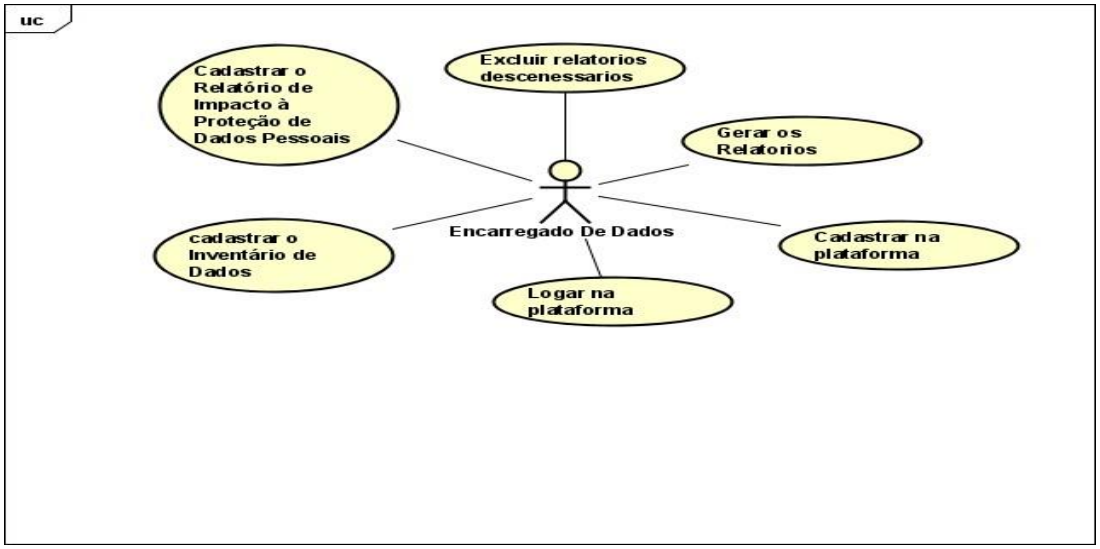
Na etapa 6, o art. 5º, XVII da LGPD preconiza que o Relatório de Impacto deve descrever “medidas, salvaguardas e mecanismos de mitigação de risco“. Antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais.

Na etapa 7, depois que os riscos estão descritos de acordo com o seu grau de probabilidade e impacto, é preciso identificar as medidas para mitigá-los. Essas medidas podem ser técnicas, de segurança ou mesmo administrativas.

Na etapa 8, o relatório deve ser registrado e aprovado, incluindo as assinaturas do responsável pela elaboração, do encarregado e dos representantes do controlador e do operador

Na etapa 9, o relatório deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pela instituição.

DIAGRAMA DE CASOS DE USO



Descrição do Caso De Uso

Quadro 2 – Caso de uso detalhado**:** Logar**.**

Caso de Uso: UC1 / Logar.

Descrição Resumida: Este caso de uso é iniciado quando o Encarregado de dados, já possui cadastro e acesso ao sistema.

Ator Primário: Encarregado de dados

Ator secundário: Servidor

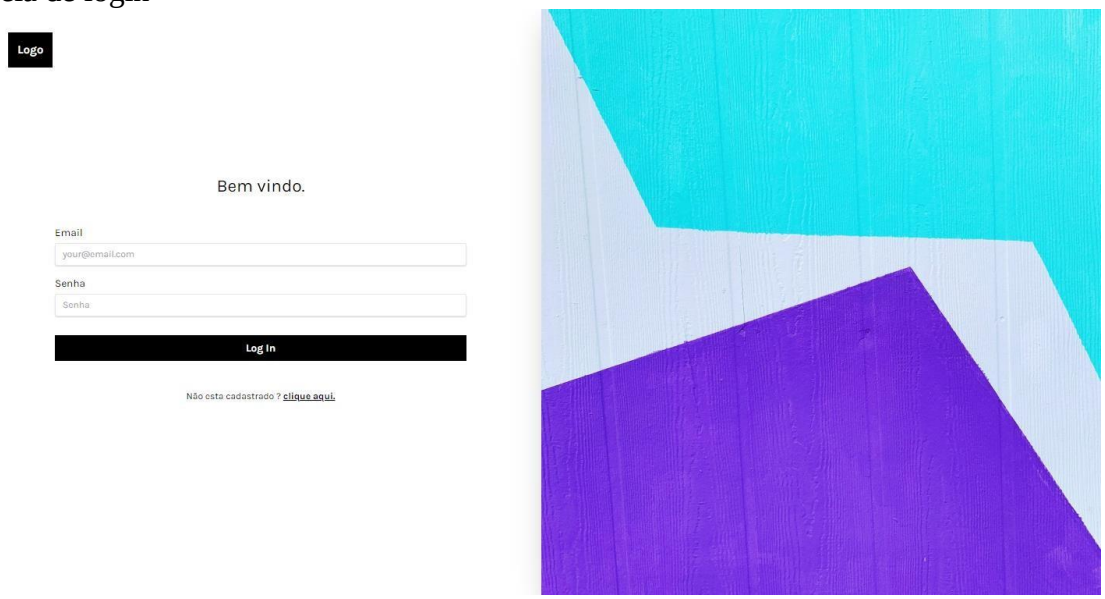
Fluxo Principal:

1- O Usuário insere o seu Email e senha e clica em Acessar
2- O servidor recebe as credenciais via HTTP e confere com as informações contidas no Banco de dados.
3- O servidor responde como sucesso caso as credenciais sejam válidas
4- O cliente acessa a página inicial do sistema
5- Encerra o caso de uso

Fluxos Alternativos:

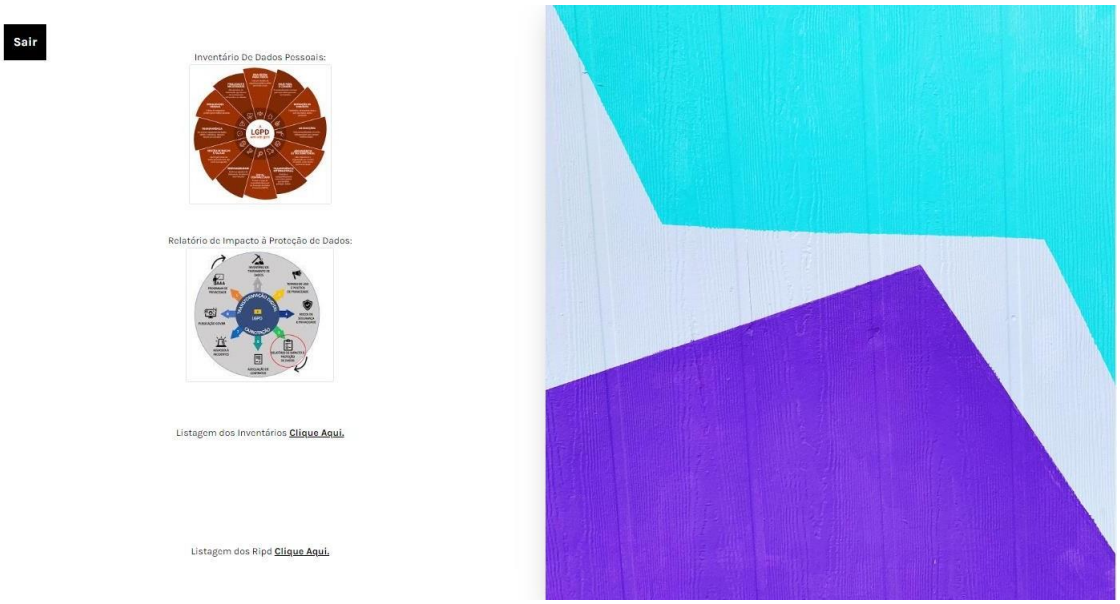
6- 3.a O Servidor responde com uma mensagem de erro de usuário ou senha.
7- 3.b retorna ao passo 1 do fluxo principal

Tela de login



fonte: Autor

Tela Home



fonte: Autor

O Encarregado clicar nos ícones

Quadro 3 – Caso de uso detalhado: Cadastrar na Plataforma**.**

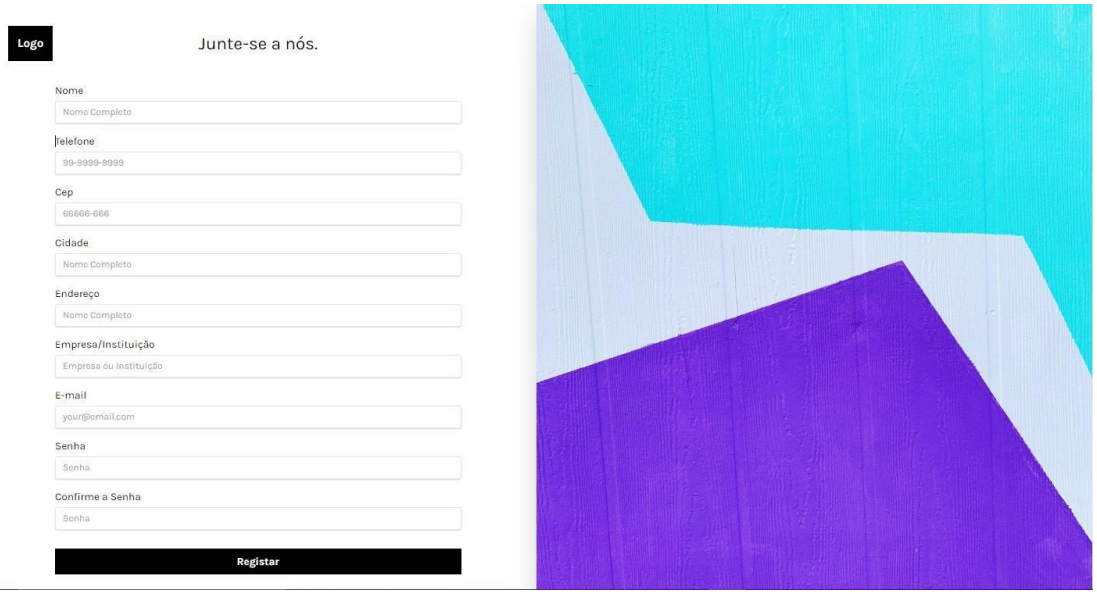
Caso de Uso: UC2 / Cadastrar na plataforma
Descrição Resumida: Este caso de uso é iniciado quando o Encarregado se cadastrar no sistema
Ator Primário: Encarregado de Dados
Ator secundário: Banco de Dados
Fluxo Principal:

1- O Encarregado de dados primeiramente disponibiliza alguns dados
2- O Encarregado de Dados escolher uma senha que será criptografada
3- Salva a senha é criptografada
3- Encerra o caso de uso

Fluxos Alternativos:

4. O Encarregado de Dados já é cadastrado na plataforma.

Tela de Cadastro

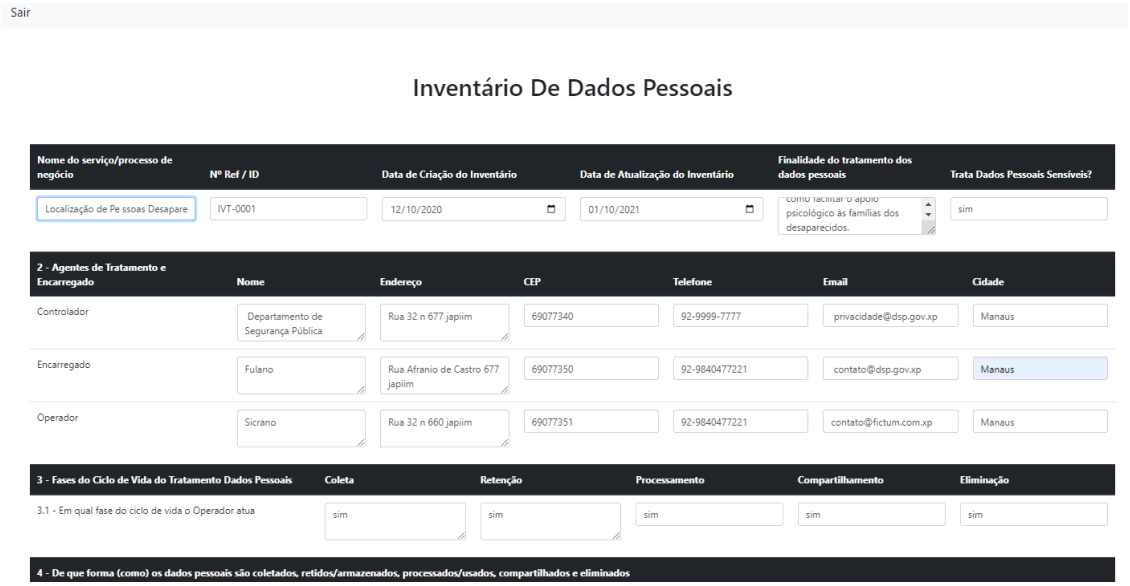


fonte: Autor

Quadro 4 – Caso de uso detalhado: Elaborar o Inventário De Dados**.**

Caso de Uso: UC 3 / Elaborar o Inventário De Dados Descrição Resumida: Este caso de uso é iniciado, quando o tratamento de dados de uma empresa é documentado. Ator Primário: Encarregado Ator secundário: Banco de dados Fluxo Principal: 1- O Encarregado faz o mapeamento dos dados 2- Cadastrar os dados no Inventário 3- Salvar o Inventário no banco de dados 4- Encarregados de Dados autorizar 5- Encerra o caso de uso Fluxos Alternativos: 6- O Encarregado excluir o Inventário De Dados

Cadastrar no banco o Inventário de Dados



fonte: Autor

O Encarregado clicar no botão salvar.

Listagem dos Inventários

fonte: Autor

O Encarregado clicar no nome dos relatórios e vai para a tela gerar inventário.

Tela para gerar o Inventário

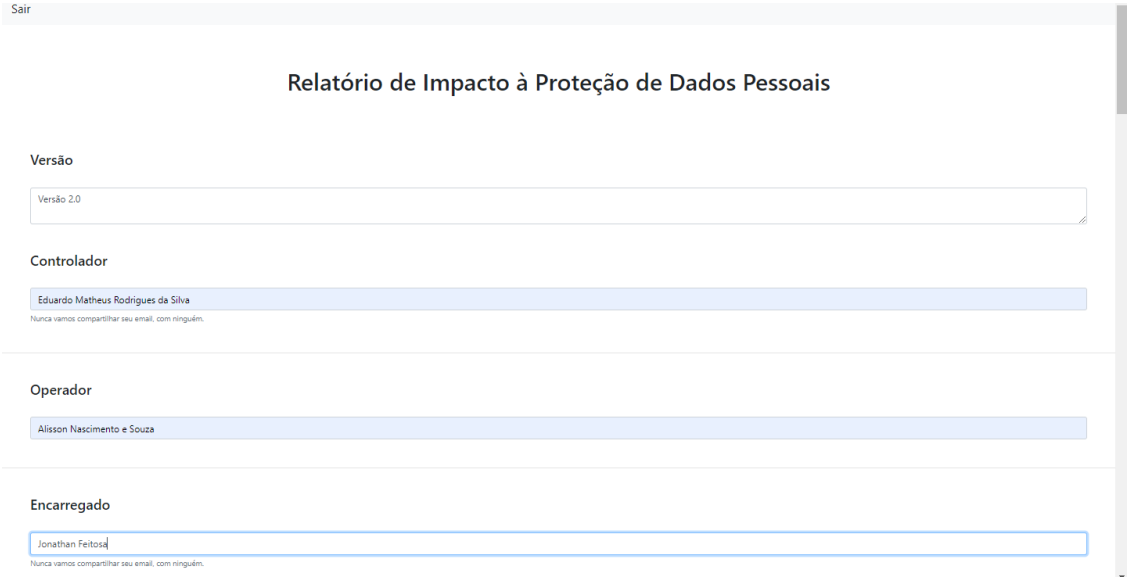
fonte: Autor

O Encarregado clicar no botão gerar relatório.

Quadro 5 – Caso de uso detalhado: Elaborar o RIPD .

Caso de Uso: UC4 / Elaborar o RIPD Descrição Resumida: Este caso de uso é iniciado, quando relatório de impacto à proteção de dados pessoais de uma empresa é feito. Ator Primário: Encarregado Ator secundário: Servidor Fluxo Principal: 1- O Encarregado a partir mapeamento dos dados, inicia o relatório 2- Cadastrar os dados do Inventário no RIPD 3- Terminar de preencher o RIPD 4- Salvar o RIPD na plataforma web 5- baixar o RIPD 6- Encerra o caso de uso

Tela RIPD



fonte: autor

Tela de listagem dos relatórios

fonte: Autor

O Encarregado faz o mesmo procedimento que nas telas do Inventário.

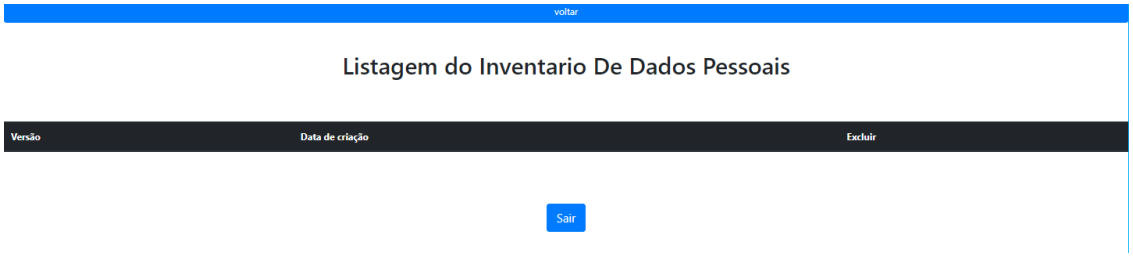
Quadro 6 – Caso de uso detalhado: Excluir Relatórios

Caso de Uso: UC5 / Excluir Relatórios Descrição Resumida: Este caso de uso é iniciado quando o Encarregado clicar em deletar Ator Primário: Encarregado de Dados Ator secundário: Banco de Dados Fluxo Principal: 1- O Encarregado logar na plataforma 2- O Encarregado ir na lista de relatórios do Ripd ou Inventário 3- O Encarregado escolher os relatórios a serem excluído 4- O Encarregado clicar em deletar 5- Encerra o caso de uso .

Relatórios deletados da listagem

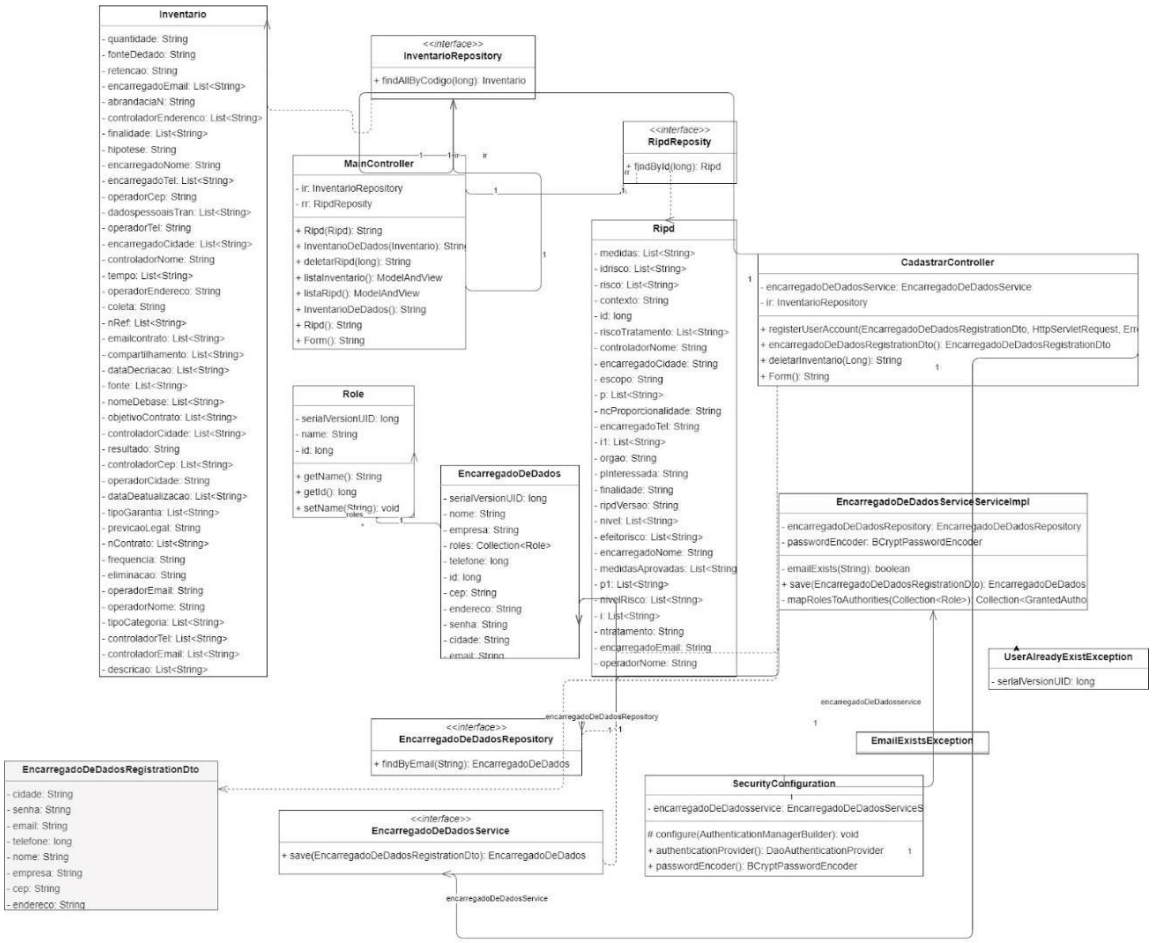
fonte: Autor

Inventários Deletados



fonte: Autor

Diagrama De Classes



Fonte: autor

Considerações Finais

A falta de soluções no mercado para facilitar as empresas a cumprirem critérios que a Lei nº 12.965 impõe, são a justificativa da pesquisa e o foco do sistema desta monografia. Além disso, existem poucos sistemas com foco na LGPD, a legislação do direito do consumidor se tornou obrigatória, e futuramente a criação dos relatórios serão essenciais ou acarretarão punições que já estão previstas em lei.

Por meio desta monografia, um sistema web foi desenvolvido para facilitar na criação dos relatórios obrigatórios da LGPD que são o RIPD e o Inventário de Dados, os requisitos desses relatórios foram definidos, e as funcionalidades foram implementadas.

Para a resolução dos problemas encontrados foram levantados alguns requisitos para a criação da plataforma, o gerador de relatório do Inventário de dados e Relatório de Impacto à Proteção de Dados, como o mesmo poderia ser utilizado pelas empresas, em sequência foi projetado uma ideia de solução, e que por final foi executado e aplicado na organização.

A plataforma possui nível de segurança garantido pelo *Spring Security*, onde o encarregado de dados se cadastrar e seus dados são protegidos e sua senha é criptografada, os relatórios são salvos no banco de dados, e os dados são exibidos em outra parte do sistema na qual, o encarregado pode visualizar relatórios que ele criou anteriormente pela plataforma, e excluir caso não seja mais necessária determinada versão, e assim gerar o arquivo pdf do relatório que desejar.

A plataforma precisa de melhorias no Design, a parte de editar cadastros dos Encarregados de Dados caso ele precise mudar algum dado como Email e um sistema de recuperação de senha.

REFERÊNCIAS

A atuação da Autoridade Nacional de Proteção de Dados (ANPD) - Migalhas. Disponível em: <https://www.migalhas.com.br/depeso/341872/a-atuacao-da-autoridade-nacional-de-protecao-de-dados-anpd>. Acesso em: 22 dez. 2021.

AUTOR, D. R. F. J. DE D. D. EM D. E.-P. DO I. - I. B. DE D. DA I. T. PUBLICADOS PELO. A Diretiva Europeia sobre proteção de dados pessoais - Jus.com.br | Jus Navigandi. Disponível em: <https://jus.com.br/artigos/23669/a-diretiva-europeia-sobre-protecao-de-dados-pessoais>. Acesso em:17 nov. 2021.

BITTAR, Carlos Alberto. Os direitos da personalidade. 8.ed., rev. aum. e mod. por Eduardo C. B. Bittar. São Paulo: Saraiva, 2015. Acesso em: 07 junho. 2022.

BOOTSTRAP: O que é, Documentação, como e quando usar. [S. l.], 25 jul. 2022. Disponível em: https://www.alura.com.br/artigos/bootstrap. Acesso em: 31 ago. 2021.

BRASIL. (Constituição 1988). Constituição da República Federativa do Brasil, Capítulo I – DOS DIREITOS E DEVERES INDIVIDUAIS E COLETIVOS, Art.5°. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso: em 15 set.2021.

BRASIL, (Código de Defesa do Consumidor), Capítulo III – DA QUALIDADE DO ATENDIMENTO, Art. 286. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6523.htm>. Acesso: em 15 set.2021.

BRASIL, (Código de Defesa do Consumidor, SEÇÃO III – Da Responsabilidade pelo Fato do Produto e do Serviço, Art.13. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm> . Acesso: em 15 set.2021.

Cambridge Analytica, GDPR - 1 year on - a lot of words and some action. Disponível em: <https://privacyinternational.org/news-analysis/2857/cambridge-analytica-gdpr-1-year-lot-words-and-some-action>. Acesso em: 10 nov. 2021.

CRESWELL, J. W. Projeto de pesquisa: Métodos qualitativo, quantitativo e misto. 3. ed. Porto Alegre: Artmed, 2010

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. Acesso em: 07 junho. 2022.

Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml>. Acesso em: 29 nov. 2021.

General Data Protection Regulation (GDPR) | Local Government Association. Disponível em:<https://www.local.gov.uk/our-support/guidance-and-resources/general-data-protection-regulation-gdpr>.Acesso em: 05 dez. 2021.

Guia da LGPD PARA EMPRESAS Desenvolvido por. [s.l: s.n.]. Disponível em: <https://www.martinezminto.com/wp-content/uploads/2020/09/Ebook-Guia-da-LGPD-para-Empresas.pdf>. Acesso em: 25 set. 2021.

Guia inventário dados pessoais.pdf — Português (Brasil). Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf/view>. Acesso em: 15 out. 2021.

Histórico das leis de proteção de dados e da privacidade na internet. Disponível em: <https://assisemendes.com.br/historico-protecao-de-dados/>. Acesso em: 27 out. 2021.

Histórico da Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://advocatta.org/historico-da-lei-geral-de-protecao-de-dados-lgpd/>. Acesso em: 18 set. 2021.

LGPD para o seu site | LGPDY. Disponível em: <https://lgpdy.com/>. Acesso em: 05 dez. 2021.

Mapeamento de Dados: O que é e como fazer data mapping. Disponível em: <https://blconsultoriadigital.com.br/mapeamento-de-dados/>. Acesso em: 03 nov. 2021.

MYSQL. MySQL Documentation. Disponível em: <https://www.mysql.com/doc/>. Acesso em: 01 out. 2021.

NACIONAL, I. PORTARIA No 11, DE 27 DE JANEIRO DE 2021 - DOU - Imprensa Nacional. Disponível em: <https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313>. Acesso em: 22 nov. 2021.

O caso Cambridge Analytica e a influência na criação da LGPD. Disponível em: <https://encript.com.br/o-caso-cambridge-analytica-e-a-influencia-na-criacao-da-lgpd/>. Acesso em: 15 out. 2021.

Oficina LGPD Inventário de Dados Pessoais Oficina Dirigida Inventário de Dados Pessoais. [s.l: s.n.]. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/apresentacoes/apresentacao_inventario_dados_pessoais.pdf>. Acesso em: 08 out. 2021.

Oficina LGPD Relatório de Impacto à Proteção de Dados Pessoais -RIPD. [s.l: s.n.]. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/apresentacoes/apresentacao_ripd.pdf>. Acesso em: 22 out. 2021.

Punições pelo uso indevido de dados pessoais começam a valer no domingo. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/07/29/punicoes-pelo-uso-indevido-de-dados-pessoais-comecam-a-valer-no-domingo>. Acesso em: 22 out. 2021.

The Law Reviews - The Privacy, Data Protection and Cybersecurity Law Review. Disponível em: <https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/germany>. Acesso em: 03 nov. 2021.

Thymeleaf. Disponível em: <https://www.thymeleaf.org/>. Acesso em: 01 out. 2021.

SILVA FILHO, Antonio Mendes da. **A Era da Informação**. Disponível em: <http://www.espacoacademico.com.br/002/02col_mendes.htm>. Acesso em: 07 dez. 2021.

Software Java. Disponível em: <https://www.oracle.com/br/java/>. Acesso em: 01 out. 2021.

SMITH, J. The History of the General Data Protection Regulation - European Data Protection Supervisor - European Data Protection Supervisor. Disponível em: <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en>.22 nov. 2021.

Spring Projects. Disponível em: <https://spring.io/projects/spring-boot>.Acesso em: 01 out. 2021.

MINISTÉRIO DA EDUCAÇÃO
INSTITUTO FEDERAL DO AMAZONAS

SOLICITAÇÃO ELETRÔNICA Nº 1132/2023 - PROT/CMC (11.01.03.01.08.08)

Nº do Protocolo: NÃO PROTOCOLADO

Manaus-AM, 10 de Fevereiro de 2023

ilovepdf_merged.pdf

Total de páginas do documento original: 62

(Assinado digitalmente em 13/02/2023 08:34)
MARIA LUZIA DA TRINDADE
VIGILANTE
267810

Para verificar a autenticidade deste documento entre em https://sig.ifam.edu.br/documentos/ informando seu número: **1132**, ano: **2023**, tipo: **SOLICITAÇÃO ELETRÔNICA**, data de Assinatura: **10/02/2023** e o código de verificação: **a2d7a47534**