

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE INFORMÁTICA
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

Sistema Interativo de Autodiagnóstico (SIA) - Um guia para adequação a
LGPD

Getúlio Carvalho Silva
Junno Lúcio Lopes Guimarães Jacob
Maria Eduarda Alves Bezerra
Rafael Oliveira De Melo

GOIÂNIA-GO,
JULHO, 2024.

Getúlio Carvalho Silva
Junno Lúcio Lopes Guimarães Jacob
Maria Eduarda Alves Bezerra
Rafael Oliveira De Melo

Sistema Interativo de Autodiagnóstico (SIA) - Um guia para adequação a LGPD

Relatório elaborado como um dos requisitos
para aprovação na disciplina INF0407 -
Residência Técnica em Sistemas de
Informação do Curso de Sistemas de
Informação da Universidade Federal de
Goiás

Professores:
Alessandro Cruvinel Machado de Araujo
Celso Gonçalves Camilo Junior
Eliomar Araújo de Lima
Nivaldo Pereira de Moraes Junior
Vagner Jose do Sacramento Rodrigues

SUMÁRIO

1 INTRODUÇÃO	3
2 DESENVOLVIMENTO	7
O CONTEXTO DA RESIDÊNCIA TÉCNICA	7
A LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA	7
OS IMPACTOS NEGATIVOS DA BAIXA CONFORMIDADE COM A LGPD	8
RELAÇÃO ENTRE A LGPD, ESG E ODS DA ONU	8
O INTERESSE E OS DESAFIOS NA ADEQUAÇÃO	9
A SOLUÇÃO PROPOSTA	10
METODOLOGIA E FERRAMENTAS	11
ARQUITETURA DA APLICAÇÃO	12
MODELO DE ARQUITETURA TÉCNICA	23
ROADMAP	26
ARQUITETURA DE NEGÓCIO	32
PROPOSTA DE CRIAÇÃO DE DAO PARA O SIA LGPD	45
3 CONSIDERAÇÕES FINAIS	53
REFERÊNCIAS	54

1. Introdução

A conformidade com a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, promulgada no Brasil em agosto de 2018 e em vigor desde setembro de 2020, representa um marco crucial para todas as entidades que lidam com informações pessoais. Esta legislação estabelece diretrizes rigorosas sobre como dados pessoais devem ser tratados, afetando tanto entidades públicas quanto privadas, e demandando um novo padrão de cuidado e responsabilidade na gestão desses dados.

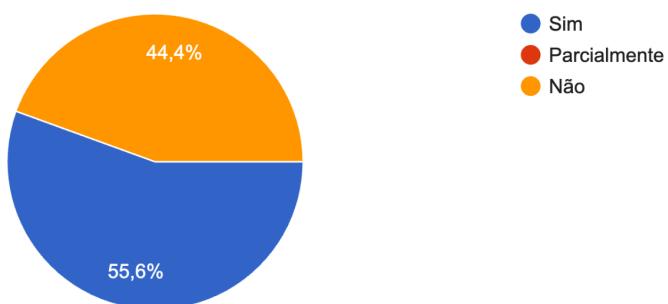
A implementação eficaz da LGPD é um desafio significativo para muitas empresas brasileiras, especialmente as de pequeno porte, que enfrentam barreiras como a falta de recursos para investimentos em capacitação especializada e adaptação de processos. De acordo com o estudo IT Trends Snapshot 2023, apenas 36% das empresas afirmam estar totalmente aderentes à legislação, evidenciando a necessidade premente de soluções acessíveis e práticas para facilitar a conformidade.

Dentro do contexto da Residência Técnica em Sistemas de Informação da UFG, buscando compreender melhor o cenário atual, desenvolvemos um formulário com o objetivo de avaliar a situação das pequenas e médias empresas em relação à conformidade com a Lei Geral de Proteção de Dados (LGPD). Este formulário visa identificar o nível de adequação dessas empresas às exigências legais, bem como suas percepções sobre os riscos e impactos associados à proteção de dados.

GRÁFICO 1 – Percentual de empresas que se consideram aderentes à LGPD

A sua empresa está em conformidade com a LGPD?

9 respostas

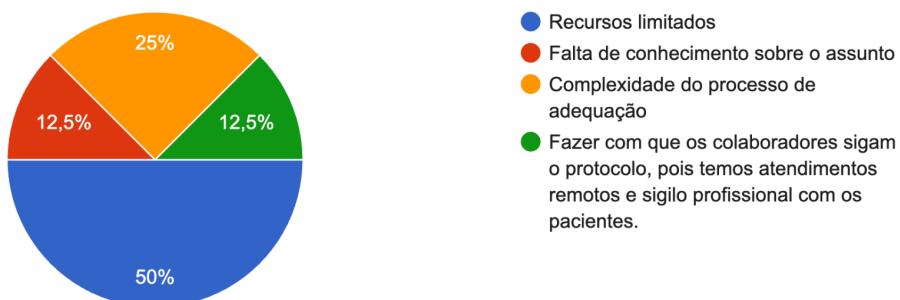


Fonte: Elaborado pelo autor.

GRÁFICO 2 – Principais desafios no processo de adequação à LGPD

Quais são os maiores problemas no processo de adequação?

8 respostas

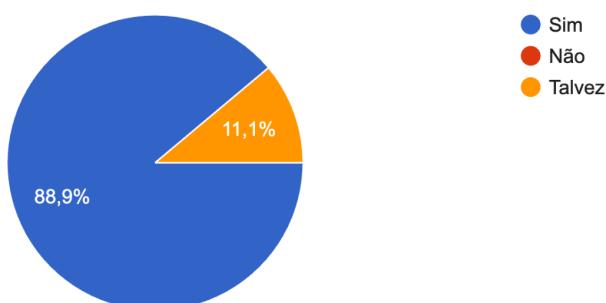


Fonte: Elaborado pelo autor.

GRÁFICO 3 – Percentual de empresas que temem sanções por não conformidade com a legislação

A empresa teme consequências da não conformidade com a LGPD?

9 respostas

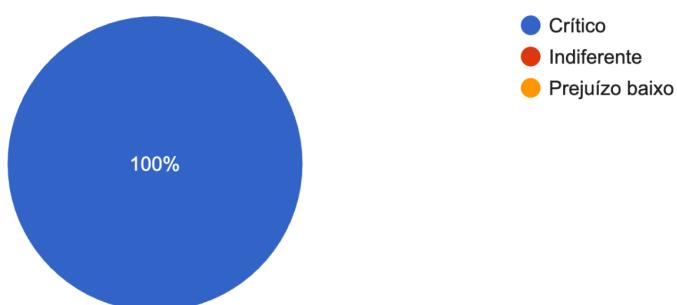


Fonte: Elaborado pelo autor.

GRÁFICO 4 – Percentual de empresas que consideram crítico o impacto de uma multa relacionada à LGPD

Como afetaria a empresa ter que pagar uma multa de 2% do faturamento do último ano em decorrência do não cumprimento da LGPD?

8 respostas



Fonte: Elaborado pelo autor.

Através desta pesquisa, coletamos informações valiosas que nos permitiram assimilar melhor os desafios enfrentados por essas empresas na implementação da LGPD, além de fornecer insights sobre suas principais preocupações e dificuldades.

Em um contexto mais amplo de governança corporativa, a adequação à LGPD se torna não apenas uma exigência legal, mas também uma componente essencial das práticas de ESG (Environmental, Social, and Governance). Empresas que adotam padrões elevados de governança, como o cumprimento rigoroso de regulamentações de proteção de dados, fortalecem sua reputação, mitigam riscos e aumentam sua atratividade para investidores e clientes conscientes.

Diante desse cenário, é proposta a criação do Sistema Interativo de Autodiagnóstico (SIA), uma plataforma inovadora desenvolvida para auxiliar pequenas empresas na jornada de adequação à LGPD. O SIA não apenas simplifica o processo de avaliação do nível de conformidade, mas também orienta as organizações na implementação das mudanças necessárias para atender aos requisitos legais. Ao fornecer uma estrutura intuitiva e acessível, o sistema permite que empresas identifiquem suas necessidades específicas de adequação e recebam orientações personalizadas, promovendo uma gestão eficiente e econômica dos recursos disponíveis.

Benefícios esperados:

1. **Redução de riscos legais e financeiros:** Ao atingir conformidade com a LGPD, as empresas diminuem significativamente o risco de multas e processos judiciais por violação de dados pessoais.
2. **Fortalecimento da confiança:** A implementação de práticas robustas de proteção de dados fortalece a confiança dos clientes, parceiros comerciais e investidores, posicionando a empresa como um parceiro confiável e ético.
3. **Melhoria da competitividade:** Empresas que se destacam pela conformidade com normas de proteção de dados ganham uma vantagem competitiva no mercado, especialmente em um contexto global cada vez mais regulado.
4. **Eficiência operacional:** O SIA permite uma gestão mais eficiente dos processos internos relacionados à LGPD, otimizando o tempo e os recursos dedicados à conformidade.
5. **Promoção da inovação responsável:** Ao integrar princípios de proteção de dados desde o desenvolvimento de novos produtos e serviços, a solução promove uma cultura de inovação responsável e sustentável.

No decorrer do trabalho discutiremos os objetivos gerais e específicos da solução, bem como as justificativas para sua realização, destacando os benefícios esperados para as empresas usuárias e a relevância do SIA no atual cenário de conformidade com a LGPD e de práticas de governança corporativa alinhadas aos princípios de ESG.

2. Desenvolvimento

O contexto da Residência Técnica

A Residência Técnica da graduação em Sistemas de Informação da Universidade Federal de Goiás é a última disciplina a ser cumprida pelos estudantes e busca inserir estes estudantes em um processo de solução de problemas reais enfrentados pela sociedade. Nesta instância da Residência, não compareceram agentes externos à UFG solicitando auxílio na resolução de seus respectivos problemas. Assim, os estudantes foram divididos em três grupos e orientados a realizar suas próprias pesquisas em busca de problemas relevantes. Foi determinado que cada um dos grupos encontrasse problemas relacionados à sigla da língua inglesa ESG, traduzida como ambiental(questões relacionadas à preservação do meio ambiente), social(questões relacionadas à desigualdade e exclusão social) e governança(questões relacionadas à governança corporativa, ética e transparência), o tema explorado neste trabalho. Também foi determinado que os problemas propostos tivessem relação com os Objetivos de Desenvolvimento Sustentável da Organização das Nações Unidas e que as soluções propostas fossem compatíveis com a criação de uma DAO (organização autônoma descentralizada). Além das determinações houve um incentivo para que as soluções beneficiassem empresas de pequeno porte.

A Lei Geral de Proteção de Dados brasileira

Considerando as determinações desta instância da Residência Técnica, o grupo responsável por este trabalho decidiu investigar a [Lei Geral de Proteção de Dados](#) (BRASIL, 2018) brasileira, suas estipulações, seus impactos, a parcela das empresas de pequeno porte adequadas e os níveis de adequação.

Com o aumento da digitalização dos aspectos da vida cotidiana, um grande conjunto de dados de variados graus de importância passou a ser controlado pelas instituições com as quais os cidadãos interagem. Dentre essas instituições estão serviços de comunicação, instituições financeiras, comércio, prestadores de serviços e órgãos públicos. Algumas dessas instituições passaram a acumular quantidades massivas de dados sensíveis que foram usados de forma inapropriada, causando danos graves como no chamado Escândalo de dados Facebook–Cambridge Analytica (BBC, 2018). Assim, se aprofundou a discussão a respeito da proteção e do uso adequado de dados de pessoas comuns.

A legislação pioneira na visão moderna de tratamento de dados pessoais foi a [GDPR](#) (UNIÃO EUROPÉIA, 2016), que definiu termos mais claros sobre as obrigações dos detentores dos dados e os direitos dos titulares. A GDPR se tornou um modelo para a criação de leis semelhantes em outros países, como a LGPD no Brasil.

De forma geral a LGPD prevê que os controladores de dados pessoais precisam de justificativas plausíveis para a existência dos seus bancos de dados, que o consentimento dos titulares dos dados deve ser obtido de forma explícita antes da coleta destes dados e que medidas adequadas devem ser tomadas para garantir a proteção dos dados. Caso a lei seja descumprida, o controlador pode sofrer punições como advertências, multas ou ser obrigado a destruir os dados.

Os impactos negativos da baixa conformidade com a LGPD

O nível geral de adequação das empresas à LGPD é baixo, com um levantamento (RD STATION, 2021) apontando que apenas 15% das empresas estava totalmente adequada e 22% não adotava nenhuma medida de segurança de dados. A adequação se torna ainda mais difícil para empresas de pequeno porte que ainda possuem muitos processos analógicos ou não completaram sua transformação digital (ABDI, 2021).

Dentre os impactos negativos que podem ser sofridos por empresas em violação da LGPD está o pagamento de multas, o custeio de advogados em processos judiciais, o pagamento de indenizações para titulares e graves danos à imagem da empresa diante da sociedade. Pesquisas (COMITÊ GESTOR DA INTERNET NO BRASIL, 2022) e incidentes (BARBOSA, 2020) (BARRETO, 2021) conhecidos demonstram que a piora da imagem de uma empresa pode trazer prejuízos financeiros reais, principalmente através de boicotes incitados por consumidores ou parceiros comerciais.

O baixo nível de adequação à LGPD pode ser especialmente danoso para empresas pequenas pois são em grande parte negócios com recursos escassos. Mesmo que possam receber tratamento diferenciado, organizações desse porte não estão imunes às punições, como evidenciado pelo caso da Telekall InforService que recebeu a primeira multa por descumprimento da LGPD (ANPD, 2023).

Relação entre a LGPD, ESG e ODS da ONU

Existe uma relação clara entre a promoção da LGPD, adesão às boas práticas de ESG e o cumprimento dos ODS da ONU. Em primeiro lugar, o próprio texto da LGPD afirma que proteger direitos fundamentais, promover o desenvolvimento econômico,

tecnológico e a inovação e garantir o exercício da cidadania são objetivos da lei. Os objetivos da LGPD estão alinhados à Declaração Universal dos Direitos Humanos que prevê em seu Artigo 12 que "Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.". A LGPD está alinhada com a Constituição Brasileira que prevê que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.". A LGPD é fundamental para o cumprimento do Estatuto da Criança e do Adolescente que prevê "privacidade: a promoção dos direitos e proteção da criança e do adolescente deve ser efetuada no respeito pela intimidade, direito à imagem e reserva da sua vida privada". Cumprir as premissas desses documentos é fundamental para atingir o ODS 16 que é a promoção de sociedades pacíficas e inclusivas, prover acesso à justiça e construir instituições efetivas. Ao promover a inovação a LGPD também apoia o ODS 9.

Há de se considerar também que no Global Risks Report 2023 do Fórum Econômico Mundial, se afirma que o uso inapropriado de dados pessoais pode desde agravar a discriminação contra populações vulneráveis até possibilitar a criação de armas biológicas. O relatório também afirma que a privacidade das pessoas está sob ataque por entidades governamentais preocupadas com a segurança pública e pela busca de vantagens econômicas. No Global Risks Report 2024 um risco global é definido como a possibilidade de ocorrência de um evento que pode causar impactos negativos em uma parte significativa do PIB, população ou recursos naturais globais. Os riscos globais enumerados incluem:

- Riscos Sociais: Erosão de direitos humanos (privacidade sendo um desses direitos);
- Riscos Tecnológicos: Censura e vigilância (supressão de direitos humanos como privacidade), Insegurança cibernética (sequestro, roubo e fraude de dados)

A LGPD pode ser efetiva na mitigação dos riscos apontados nos dois Global Risks Report citados. Esses riscos são ameaças ao cumprimento dos ODS 3, 5, 10 e 16.

Por fim, a LGPD está alinhada com os Princípios para a Governança e Uso da Internet no Brasil, formulados pelo Comitê Gestor da Internet no Brasil. Isto significa que a LGPD avança a implementação das melhores práticas de governança no Brasil, fortalecendo a relação com o aspecto de governança de ESG.

O interesse e os desafios na adequação

Embora os níveis de adequação sejam baixos, especialmente para empresas pequenas, muitos empresários reconhecem que a LGPD é uma mudança positiva (RD

STATION, 2021) (COMITÊ GESTOR DA INTERNET NO BRASIL, 2022) e que melhorias na governança trazem bons resultados(BELARMINO, 2020). Existem inúmeras soluções que facilitam a adequação como consultorias especializadas, cursos, treinamentos e ERPs. O que poderia então explicar a baixa adequação? Através da pesquisa e das discussões realizadas com empresas locais foram encontrados os seguintes desafios:

- Custo: os donos afirmam que não existe dinheiro suficiente para pagar pelas soluções existentes. Usando como referência as consultorias especializadas, que seriam a solução ideal para a maioria das empresas, em 2020 se cobrava cerca de R\$20.000,00 pelo serviço (CAMPOS JR, 2020), muito além do alcance da maioria dos empresários.
- Tempo: na visão dos administradores a adequação demandaria muito tempo que poderia ser utilizado em outras questões mais urgentes (RD STATION, 2021).
- Recursos humanos: não existe pessoal em número suficiente ou com as qualificações necessárias para fazer a adequação (RD STATION, 2021)(COMITÊ GESTOR DA INTERNET NO BRASIL, 2022).
- Falta de conhecimento: empresários disseram que não dominam o conhecimento a respeito da legislação e do processo de adequação, além de considerarem difícil a aquisição destes (RD STATION, 2021) (COMITÊ GESTOR DA INTERNET NO BRASIL, 2022).
- Complexidade: os empresários consideram o processo de adequação muito complexo para ser feito em suas empresas (RD STATION, 2021).

A solução oferecida para esses empresários deve remover os obstáculos citados acima para que a sua chance de sucesso seja maior.

A solução proposta

Após a realização do processo de pesquisa, discussões com empresas locais, consolidação e análise dos dados coletados, é proposta a criação de um sistema digital para auxiliar empresas de pequeno porte a se adequarem à LGPD. Existem soluções no mercado para fazer a adequação, mas por um ou vários motivos citados anteriormente elas não atendem às necessidades das empresas pequenas. Para os usuários finais, o sistema deve ser barato, não demandar conhecimentos extensos de direito, segurança digital, governança, além de compartmentalizar e abstrair as complexidades envolvidas no processo de adequação. Como o tempo disponível para a realização das tarefas da

residência não é suficiente para a criação de um produto final, neste documento é desenvolvido um projeto que vai direcionar a implementação completa da solução proposta. Apesar disso, foi tentada a construção de artefatos que mais se aproximam do objetivo do projeto, como protótipos funcionais que podem ser acessados em um navegador de internet.

Metodologia e ferramentas

O projeto foi executado e gerenciado utilizando a metodologia Scrum, uma abordagem ágil que organiza o trabalho em ciclos curtos e iterativos chamados sprints. Essa metodologia permitiu à equipe trabalhar de forma mais flexível e colaborativa, adaptando-se às mudanças ao longo do processo. Em cada sprint a equipe planejou, desenvolveu e revisou um conjunto específico de tarefas e objetivos, garantindo que o trabalho fosse realizado de maneira eficiente.

Para a construção do projeto, foi necessária a utilização de diversas ferramentas para coleta de dados, gestão de tarefas e criação de documentos. Essas ferramentas facilitaram a comunicação e organização da equipe, assegurando que todos estivessem alinhados e que as tarefas fossem executadas como o planejado.

Gestão de projeto

- Gestão de tarefas: Product Backlog, Google Meet, Whatsapp
- Versionamento e repositório: [Github](#) e [Google Drive](#)

Mapeamento inicial

- Reuniões de Brainstorming
- Coleta de dados: Entrevistas presenciais, Google Forms, Google Planilhas

Produção de artefatos

- Documentos: Google Docs, Canvas, Google Planilhas
- Diagramas: Draw.io
- Protótipos: Figma

Arquitetura da aplicação

Requisitos funcionais

Através dos requisitos funcionais, são descritas as funcionalidades que o Sistema Interativo de Autodiagnóstico oferece para atender às necessidades dos clientes e aos objetivos do negócio.

RF01 - Cadastrar dados gerais dos usuários: Para todos os perfis de usuário (Administrador, Encarregado e Colaborador), o sistema deve permitir cadastrar via formulário os seguintes dados em comum: nome completo, CPF, data de nascimento, endereço, e-mail e telefone para contato. O sistema também deve registrar automaticamente a data de cadastro de cada usuário.

RF02 - Cadastrar dados específicos de colaboradores e encarregados: para usuários colaboradores e encarregados, o sistema deve permitir cadastrar, no mesmo formulário de cadastro do **RF01**, os seguintes dados: código do funcionário (caso exista na organização) cargo, departamento e data de admissão.

RF03 - Cadastro de usuário administrador: O sistema deve permitir realizar o cadastro do usuário administrador. Em geral, este pode corresponder ao gestor da empresa ou ao sócio-administrador. As credenciais de acesso (nome de usuário, senha e token de aplicativo de autenticação) devem ser geradas pela equipe de implantação/desenvolvimento/suporte do sistema e fornecidas diretamente à pessoa responsável. O administrador, por sua vez, poderá acessar e preencher o formulário com os dados cadastrais (**RF01**).

Desde que autorizado dentro da organização, o indivíduo com o perfil de acesso encarregado também pode ter credenciais de acesso para o perfil de administrador.

RF04 - Cadastro de usuário encarregado: O sistema deve permitir realizar o cadastro do usuário encarregado. Este será o responsável por gerenciar o processo de implementação da adequação da empresa à LGPD. As credenciais de acesso (nome de usuário, senha e token de aplicativo de autenticação) também devem ser geradas pela equipe de implantação ou de desenvolvimento do sistema. O encarregado, ao acessar o sistema, poderá preencher o formulário de dados cadastrais (**RF01** e **RF02**).

RF05 - Cadastro de usuários colaboradores: O usuário encarregado deverá ser capaz de cadastrar o usuário colaborador que fará parte da adequação. Ele deverá preencher o formulário de cadastro do colaborador (**RF01** e **RF02**), gerar o nome de acesso, o token de aplicativo de autenticação e uma senha provisória para o colaborador (que poderá alterá-la no primeiro acesso).

RF06 - Cadastro de empresa: O usuário administrador deverá ser capaz de cadastrar inicialmente a sua organização que será alvo da adequação pretendida pelo sistema.

O cadastro deve conter as informações de: CNPJ, razão social, nome fantasia, ramo de atuação (CNAE Principal), data de fundação, e-mail, telefone para contato, endereço e dados do(s) gestor(es)/sócio-administradores (onde os dados do próprio administrador podem ser preenchidos automaticamente a partir dos dados que foram cadastrados previamente para o seu usuário).

RF07 - Autenticar usuário: Tanto o usuário administrador, como o encarregado e o colaborador só poderão acessar o sistema após a autenticação, informando o nome de usuário, senha e o código fornecido por um aplicativo de autenticação.

RF08 - Recuperar acesso: caso o usuário colaborador não consiga realizar a autenticação, este deve solicitar ao administrador ou encarregado a criação de nova senha provisória e/ou token para o aplicativo de autenticação. O sistema deve permitir que o encarregado gere a nova senha provisória e o token. Caso o acesso precise ser recuperado para administrador ou encarregado, será necessário entrar em contato com o suporte via telefone ou e-mail.

RF09 - Realizar logout: O sistema deve permitir que o usuário realize o logout, sendo necessário autenticar-se outra vez para acessar novamente.

RF10 - Preencher formulário de autodiagnóstico: O sistema deve permitir que o usuário encarregado pela implementação da adequação preencha o formulário de autodiagnóstico.

RF11 - Visualizar resultado do nível de conformidade atual: a partir do formulário preenchido, o sistema deve calcular e emitir o resultado do nível de conformidade atual da empresa, exibindo o diagrama de etapas de nível de maturidade (de 1 a 5), contendo o grau de conformidade alcançado e também destacando as áreas que necessitam de melhorias para aumentar esse grau.

RF12 - Visualizar etapas pendentes e etapas que já foram realizadas: O usuário encarregado deve ser capaz de visualizar além do diagrama citado no **RF11**, as etapas de adequação que ele já concluiu bem como as que estiverem pendentes para que sua organização evolua para um próximo nível de maturidade.

RF13 - Visualizar materiais de referência e ferramentas recomendadas: O sistema deve permitir que o usuário visualize materiais de referência, tais como artigos, guias práticos e modelos de políticas (em PDF, armazenados nos servidores do sistema e exibidos diretamente na tela), links úteis (abertos em uma nova aba) e sugestões de ferramentas recomendadas, contendo o nome, breve descrição e links oficiais para mais informações (abertos em uma nova aba).

RF14 - Visualizar gráficos e diagramas de acompanhamento (Dashboards): O usuário encarregado deve ser capaz de visualizar os gráficos e diagramas contendo as informações que permitem analisar o desempenho da adequação até então, estando estas no Dashboard de Conformidade, e sendo: o diagrama de etapas de nível de maturidade (**RF11**) que serve como um guia e referência; e o histórico de atividades realizadas em um determinado período definido via filtro (dia, mês e ano iniciais e finais); e no Dashboard de Treinamento,

sendo: o gráfico indicando os cursos realizados pelos colaboradores; e o gráfico indicando a quantidade mensal de colaboradores que realizaram os cursos (filtrado por mês e ano).

Demais informações podem ser exibidas em gráficos e diagramas de acordo com aprimoramentos e evoluções do sistema ou possíveis alterações referentes à LGPD, por exemplo.

RF15 - Visualizar os cursos disponibilizados pelo sistema: O usuário encarregado deve ser capaz de visualizar a lista de cursos em vídeo disponibilizados pelo sistema. Para cada vídeo, o sistema deve exibir a sua thumbnail (“miniatura”, ou “capa”), título, duração e descrição. Os vídeos (armazenados nos servidores do sistema) devem ser exibidos em player interno.

RF16 - Disponibilizar curso para colaborador: O usuário encarregado deve ser capaz de disponibilizar cursos para o colaborador. Ele poderá escolher determinados cursos e alojar para determinados colaboradores.

RF17 - Visualizar cursos realizados, pendentes e iniciar um novo curso: O usuário colaborador deve ser capaz de visualizar a lista de cursos que já foram concluídos por ele, como também os que ainda estão pendentes de serem realizados. Deve também poder iniciar um novo curso.

RF18 - Acessar o suporte: Os usuários deverão ser capazes de solicitarem suporte via chat online para tirar dúvidas referente ao SIA.

RF19 - Gerar logs de acesso: O sistema deve gerar logs de acesso contendo o histórico de uso do sistema por sessão do usuário. Deve disponibilizá-los somente ao usuário administrador. O usuário encarregado pode ter esta permissão, caso autorizado pelo administrador.

Requisitos Não-funcionais

Os requisitos não funcionais definem como o Sistema Interativo de Autodiagnóstico deve se comportar, abrangendo aspectos como desempenho, segurança, usabilidade e confiabilidade, para garantir uma experiência eficiente e segura para os usuários.

RNF01 - Conformidade com a LGPD: Por se tratar do processo de adequação à LGPD e por armazenar informações sensíveis de negócio relacionadas principalmente à segurança da organização, o sistema deve assegurar a conformidade com todas as regulamentações e normas da LGPD, bem como o uso e armazenamento seguro de todos os dados com os quais irá operar e armazenar.

RNF02 - Segurança dos dados: O sistema deve proteger os dados inseridos pelos usuários, bem como solicitar permissão para processamento de seus dados e apresentação

em gráficos, dashboards, tabelas, acompanhamento e monitoramento, tudo de acordo com os requisitos legais da LGPD. Os recursos e ações de segurança precisam ser eficazes e robustos.

RNF03 - Criptografia: associado à Segurança dos Dados, o sistema deve prover a criptografia dos dados sensíveis, seja na transferência como no armazenamento.

RNF04 - Anonimização: também associado à Segurança dos Dados, os dados pessoais devem ser armazenados de forma anonimizada, preservando a identidade dos usuários.

RNF05 - Consentimento de uso dos dados: O sistema deve solicitar e registrar o consentimento feito por parte dos usuários para armazenar e operar sobre os dados pessoais dos mesmos.

RNF06 - Integridade dos dados: Os dados armazenados pelo sistema devem manter sua consistência, precisão e completude.

RNF07 - Backup e recuperação de dados: O sistema deve ser capaz de realizar backup, bem como recuperar informações, garantindo que sua funcionalidade e seus dados sejam preservados diante de eventos inesperados, sejam recuperados e estejam disponíveis.

RNF08 - Autenticação de dois fatores: A autenticação para acesso ao sistema deve ser segura, robusta e utilizar-se dos recursos de autenticação em dois fatores (por aplicativo autenticador) e uso de senha forte (com mínimo de 12 caracteres, usando caracteres especiais, números, letras maiúsculas e minúsculas).

RNF09 - Controle de acesso: Deve haver o controle de acesso de usuários, assegurando que cada perfil de usuário possa acessar somente os dados e recursos permitidos.

RNF10 - Logs de Acesso: Os logs de acesso gerados devem ser armazenados pelo período mínimo de 5 anos, de forma segura e acessados somente por pessoal autorizado, conforme citado na seção dos Requisitos Funcionais. Este recurso facilita a realização de auditorias e investigação de erros e possíveis incidentes.

RNF11 - Recuperação de acesso: Somente usuários administradores ou encarregados poderão alterar a senha de primeiro acesso de colaboradores e gerar tokens para aplicativos de autenticação.

RNF12 - Escalabilidade do sistema: O sistema deve ser capaz de suportar o aumento de usuários e de dados sem perda de desempenho, considerando que as PMEs estarão em processo de crescimento.

RNF13 - Disponibilidade dos dados: O sistema deve ser dinâmico e apresentar os dados com um tempo de resposta ótimo. Estes devem estar disponíveis sempre que necessário, tais como os resultados e as métricas que os usuários desejem visualizar.

RNF14 - Disponibilidade do sistema: O sistema deve estar sempre disponível (24h/dia, 7 dias por semana) e funcionando corretamente pela maior parte do tempo. É importante salientar essa disponibilidade, pois o início de diversas MPEs no mercado pode exigir maior tempo de trabalho, ajustes e aquisição de conhecimento por parte dos encarregados, administradores e sócio-administradores.

RNF15 - Desempenho do sistema: As solicitações dos usuários (envio de formulários, navegação pelos itens de menu, visualização de métricas, gráficos e diagramas) devem ser respondidas de forma eficiente e em tempo hábil (tendo o retorno esperado em no máximo 3 segundos).

RNF16 - Desempenho de tempo de carregamento dos vídeos e materiais de apoio: tanto os vídeos como os materiais de referência devem ser carregados e exibidos rapidamente, tornando mínimo o tempo de espera do usuário.

RNF17 - Qualidade de reprodução dos vídeos: A qualidade de reprodução dos vídeos deve ser adequada de modo a preservar a resolução original, evitar e mitigar distorções e interrupções.

RNF18 - Interface amigável: O sistema deve ter boa usabilidade, com uma interface intuitiva, de baixa curva de aprendizado e fácil de navegar, tanto para os usuários encarregados, como para os usuários colaboradores (cujo o nível de conhecimento técnico pode ser menor em relação aos encarregados).

RNF19 - Sistema responsivo: A interface do sistema deve adaptar aos diferentes tipos de dispositivos e resoluções de exibição (telas de monitores, celulares e tablets, por exemplo), mantendo a sua usabilidade e correto funcionamento.

RNF20 - Consistência: O sistema deve prover consistência da interface e da linguagem utilizada em todo o seu domínio.

RNF21 - Linguagem clara: O sistema deve utilizar uma linguagem clara e acessível, de modo a possibilitar a compreensão de termos técnicos e legais para diferentes níveis de conhecimento por parte dos usuários.

RNF22 - Manutenibilidade: O sistema deve ser desenvolvido de modo a possibilitar a ágil implementação de novas funcionalidades, correção de bugs e melhorias no próprio código, sendo fácil de manter, alterar e atualizar.

RNF23 - Código modular: O sistema deve ter seu código modular, comprehensível e com boa documentação, de modo que as modificações (correções e adição de recursos) necessárias sejam feitas de maneira rápida e prática.

RNF24 - Compatibilidade com navegadores: Por se tratar de um Sistema Web, este deve ser compatível com os diversos browsers utilizados no mercado, tais como: Google Chrome, Mozilla Firefox e Microsoft Edge.

RNF25 - Plataforma da aplicação: A plataforma principal da aplicação será a web.

RNF26 - Integração com aplicativos de autenticação: O sistema deve prover a capacidade de integração com aplicativos de autenticação, tais como o Google Authenticator.

RNF27 - Segurança de acesso à rede: A rede de comunicação entre o sistema e o servidor deve ser protegida por firewall e por aplicações de detecção de tentativas de invasão.

RNF28 - Escalabilidade da rede: A rede de comunicação deve ser escalável de modo a conseguir atender o crescimento esperado das PMEs e, consequentemente do sistema, nos próximos 5 anos.

RNF29 - Redundância: Os servidores devem ser configurados de modo a prover a alta disponibilidade, utilizando-se do recurso de redundância tanto de hardware e software quanto dos dados armazenados.

RNF30 - Segurança de acesso aos servidores: Os servidores devem ter firewall configurado e aplicações para detectar e bloquear tráfego não autorizado.

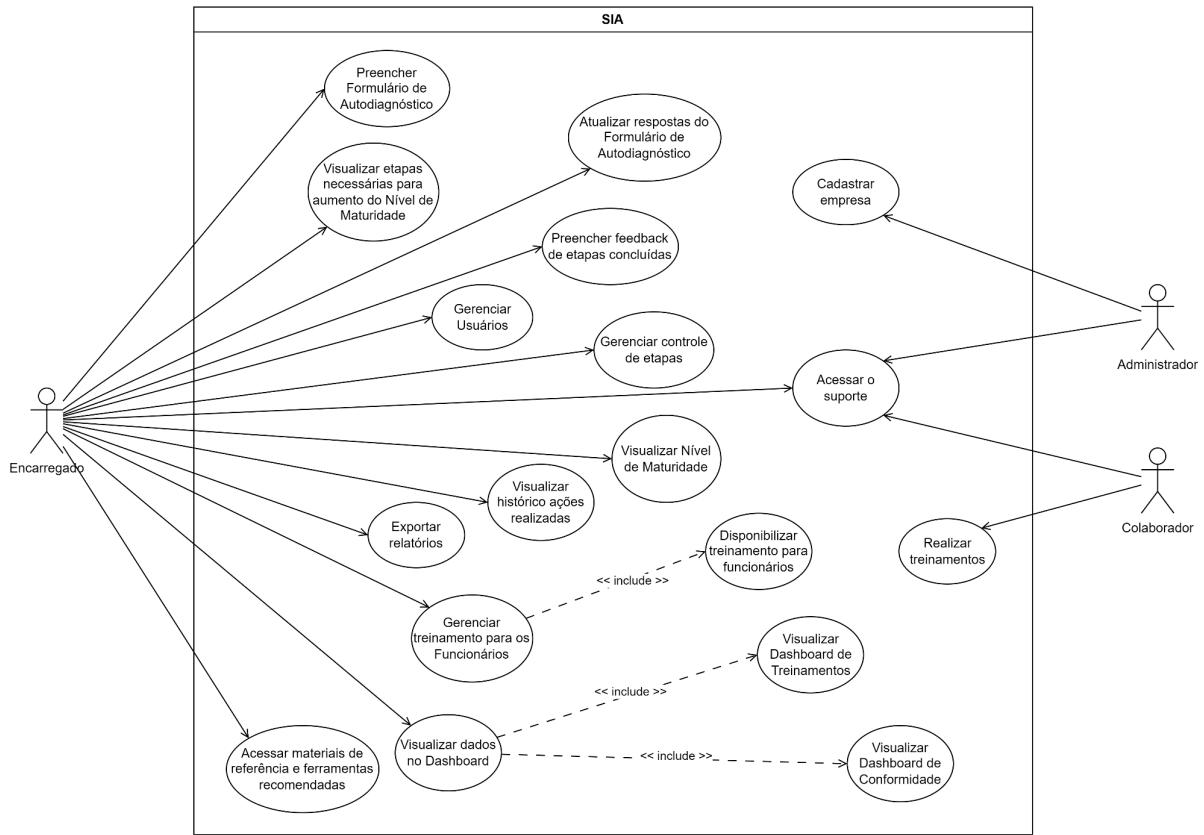
RNF31 - Suporte a testes e desenvolvimento: Os servidores devem ser compatíveis com plataformas, recursos e ferramentas de testes e de desenvolvimento.

Casos de uso

Para representar visualmente as interações que cada ator poderá realizar com o sistema, utilizamos o diagrama de caso de uso.

Obs.: o usuário administrador poderá atuar em todos os casos de uso. Evidenciamos no diagrama aqueles que são exclusivos para este ator.

Link: [Diagrama de Casos de Uso](#)



Fonte: Elaborado pelo autor.

Histórias de Usuário

Criamos histórias de usuário para capturar os requisitos do sistema do ponto de vista do usuário final. Isso ajuda a equipe de desenvolvimento a compreender de forma clara e concisa quais funcionalidades precisam ser implementadas, garantindo que o produto final atenda às necessidades e expectativas dos usuários.

Link: [Histórias de Usuário](#)

História de Usuário 1	Cadastrar Empresa
Como administrador, eu quero cadastrar uma nova empresa no sistema para que eu possa iniciar o processo de avaliação de conformidade com a LGPD.	
História de Usuário 2	Preencher Formulário de Autodiagnóstico

	Como encarregado pela conformidade, eu quero inserir dados sobre as práticas de proteção de dados da empresa para que o sistema possa avaliar nosso nível de conformidade com a LGPD.
História de Usuário 3	<p>Visualizar Nível de Maturidade</p> <p>Como encarregado pela conformidade, eu quero visualizar o nível de maturidade definido a partir do cálculo feito pelo sistema com base nos dados inseridos para que eu possa ter uma visão clara de onde precisamos melhorar.</p>
História de Usuário 4	<p>Visualizar Etapas Necessárias Para Aumento do Nível de Maturidade</p> <p>Como encarregado pela conformidade, eu quero que o sistema disponibilize de acordo a análise do nosso nível de conformidade as etapas que precisam ser executadas para que eu possa aumentar o nível de conformidade da nossa empresa com a LGPD.</p>
História de Usuário 5	<p>Acessar Materiais de Referência e Ferramentas Recomendadas</p> <p>Como encarregado pela conformidade, eu quero que nas etapas esteja descrito como posso implantá-la na minha empresa e quais materiais de referência e ferramentas podem me auxiliar nesse processo para que a implantação seja prática e facilitada.</p>
História de Usuário 6	<p>Gerenciar Controle de Etapas</p> <p>Como encarregado pela conformidade, eu quero controlar quais etapas já foram concluídas para que eu possa ter uma visão atualizada do que ainda está pendente e o resultado no nível de conformidade.</p>
História de Usuário 7	<p>Preencher Feedback de Etapas Concluídas</p> <p>Como encarregado pela conformidade, eu quero realizar feedbacks das etapas que já foram concluídas para que eu possa dar um respaldo sobre como foi o processo de implantação da etapa e nível de complexidade.</p>

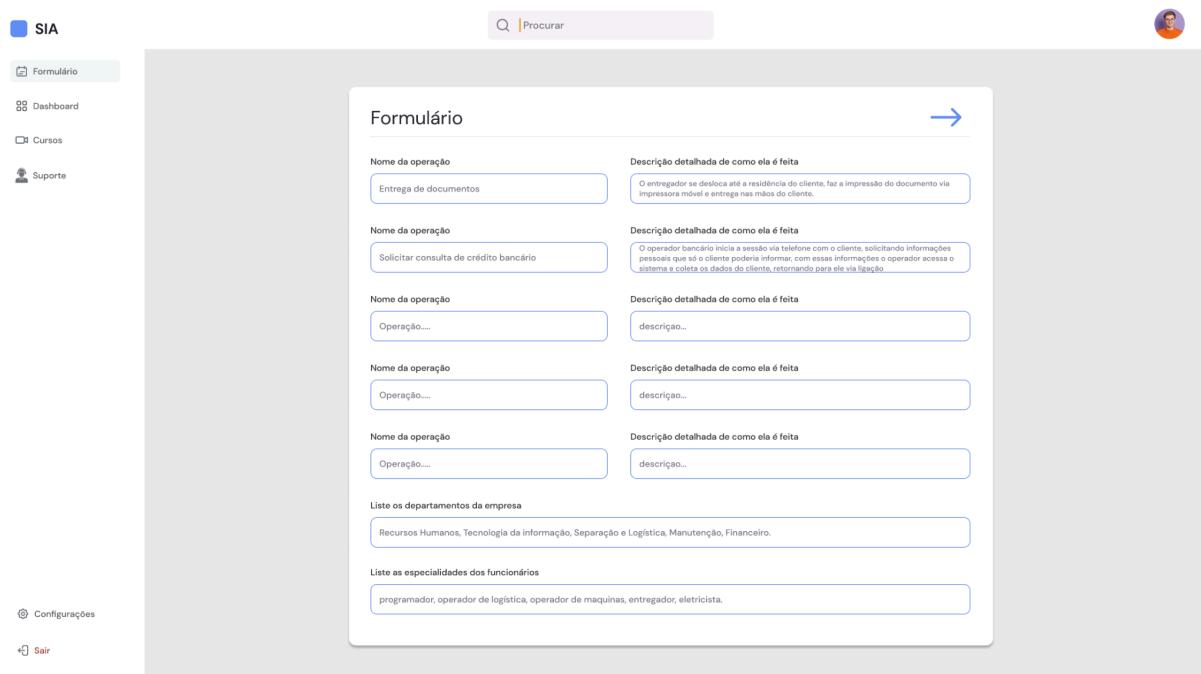
História de Usuário 8	<p>Gerenciar Usuários</p> <p>Como encarregado pela conformidade, eu quero gerenciar os usuários que têm acesso ao sistema para que eu possa controlar quem pode visualizar e editar as informações de conformidade ou acessar os cursos e materiais didáticos.</p>
História de Usuário 9	<p>Exportar Relatórios</p> <p>Como encarregado pela conformidade, eu quero exportar os relatórios de conformidade e de treinamento em formatos como PDF e Excel para que eu possa compartilhar esses relatórios com outras partes interessadas.</p>
História de Usuário 10	<p>Atualizar Respostas do Formulário de Autodiagnóstico</p> <p>Como encarregado pela conformidade, eu quero que o sistema me permita atualizar respostas do formulário para que eu possa manter as respostas corretas e atualizadas.</p>
História de Usuário 11	<p>Disponibilizar Treinamento para os Funcionários</p> <p>Como encarregado pela conformidade, eu quero configurar a disponibilização dos treinamentos sobre a LGPD, especialmente os cursos em vídeo, para os funcionários para que eu possa garantir que todos estão realizando os treinamentos corretos e no período adequado.</p>
História de Usuário 12	<p>Gerenciar Treinamento de Funcionários</p> <p>Como encarregado pela conformidade, eu quero registrar e monitorar os treinamentos sobre a LGPD realizados pelos funcionários para que eu possa garantir que todos estão cientes das suas responsabilidades em relação à LGPD.</p>
História de Usuário 13	<p>Realizar Treinamento</p> <p>Como colaborador, eu quero acessar e realizar os treinamentos disponibilizados para que eu atestar o meu próprio conhecimento e ciência quanto às práticas e regulamentos definidos pela LGPD.</p>

História de Usuário 14	<p>Visualizar Histórico de Ações Realizadas</p> <p>Como encarregado pela conformidade, eu quero acessar o histórico de conformidade e as ações tomadas em cada etapa para que eu possa realizar uma auditoria completa das práticas de proteção de dados alteradas na empresa.</p>
História de Usuário 15	<p>Visualizar dados no Dashboard</p> <p>Como encarregado pela conformidade, eu quero visualizar dados no formato de gráficos, diagramas, texto e demais recursos visuais apropriados no Dashboard para que eu possa ter uma visão tanto holística como precisa das métricas do processo de conformidade e com relação aos treinamentos realizados.</p>
História de Usuário 16	<p>Visualizar Dashboard de Conformidade</p> <p>Como encarregado pela conformidade, eu quero visualizar um dashboard com o status de conformidade da empresa para que eu possa obter uma visão geral rápida e identificar áreas que precisam de atenção imediata.</p>
História de Usuário 17	<p>Visualizar Dashboard de Treinamentos</p> <p>Como encarregado pela conformidade, eu quero visualizar um dashboard com o status de conclusão dos treinamentos para que eu possa obter uma visão geral da aderência dos funcionários aos treinamentos.</p>
História de Usuário 18	<p>Acessar o Suporte</p> <p>Como usuário, eu quero contactar o suporte para que eu possa sanar dúvidas de processos e sobre a plataforma.</p>

Protótipo de Interfaces Figma

Os protótipos foram desenvolvidos para garantir uma visão mais clara das principais funcionalidades do projeto e como seria a interface gráfica do produto final. Nele esboçamos o layout das telas de uma forma agradável ao usuário final.

Link: [Projeto no Figma](#)



Fonte: Elaborado pelo autor.

Protótipo Web Funcional:

Temos disponível no link abaixo, o link para acessar a versão Web do protótipo, contendo algumas de suas funcionalidades.

Link: [Protótipo Web Funcional](#)

Experiência e Interface de Usuário (UX/UI)

A interface do sistema busca ser o mais simples possível, indicando de forma clara o fluxo de uso para o usuário, evitando a poluição com muitas informações horizontalizadas.

A navegação com menus e botões segue um mesmo padrão, tornando mais agradável ao usuário.

O mesmo padrão é mantido também para os HEADERS (cabeçalhos), mantendo a ideia de hierarquia visual.

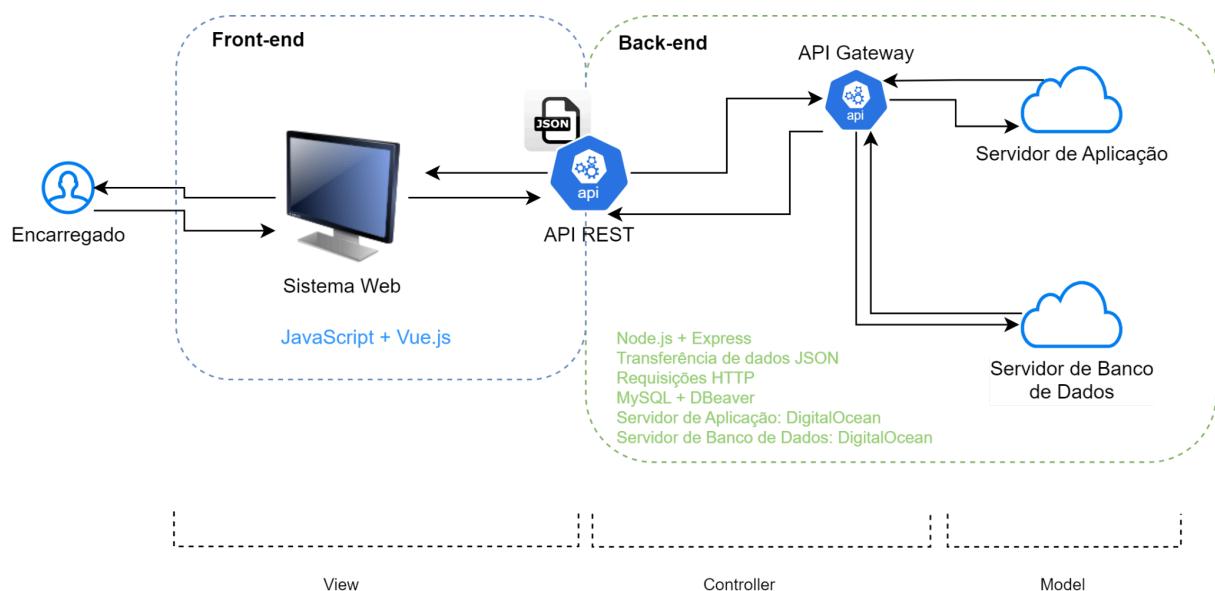
O layout é responsivo para diversas dimensões de tela.

Foi utilizado também a ideia de contraste de cores para deixar claro ao usuário qual é o principal conteúdo de cada tela.

Modelo de Arquitetura Técnica

Com a solução definida, buscamos ferramentas que fariam parte do seu desenvolvimento. Construímos um modelo de arquitetura técnica para representar de forma detalhada a estrutura, os componentes e as interações do sistema.

Link: [Modelo de arquitetura técnica](#)



Modelo de Arquitetura Técnica
Fonte: Elaborado pelo autor.

Cliente-Servidor

A arquitetura do sistema será baseada no Modelo Cliente-Servidor, sendo o navegador o Cliente, que executará a aplicação, e os Servidores os responsáveis por fornecer os serviços solicitados pelos clientes, hospedar a aplicação e a base de dados.

A escolha deste modelo justifica-se por visar atender e contribuir para o cumprimento dos seguintes requisitos levantados (podendo se estender aos demais ao longo das iterações):

- **Segurança e Privacidade:**

- **RNF02, RNF03, RNF05, RNF09, RNF10:** com a gestão de dados centralizada no servidor, o que é possibilitado por este modelo, torna-se mais fácil implementar medidas de segurança robustas, é possível realizar a

- criptografia de dados em transferência e armazenados, manter os registros (logs) de uso detalhados e utilizar-se de mecanismos de controle de acesso aos dados.
- **RNF29:** com a redundância dos servidores, o sistema continua funcionando e mantém sua disponibilidade mesmo em caso de falhas.
- **Usabilidade:**
- **RNF18, RNF19, RNF20, RNF21:** com a lógica de negócio complexa sendo centralizada no servidor a interface do usuário pode ser simplificada e otimizada para diversos navegadores e dispositivos.

Padrão Arquitetural MVC

O sistema utilizará o padrão MVC (Model-View-Controller) para organizar a lógica de aplicação nas camadas de:

- **Visão (View):** interface do usuário, na qual este irá preencher os formulários, realizar treinamentos e visualizar as métricas, por exemplo.
- **Controlador (Controller):** intermediário entre a camada de Visão e de Modelo. É responsável por receber as entradas do usuário no SIA, atualizar os dados e definir a interface a ser exibida;
- **Modelo (Model):** camada de dados da aplicação. Nesta camada estarão as regras de negócio, os dados e a lógica de manipulação dos mesmos. É nela que será realizado o cálculo para definir o nível de conformidade, por exemplo, que ocorrerá a interação direta com o banco de dados.

Front-end

JavaScript com React

- O JavaScript é a linguagem de script mais disseminada entre os browsers, o que faz com que o sistema possa ser projetado e acessado sem considerar tantas distinções entre os navegadores.
- O React possui recursos que permitem o rápido carregamento e tempo de resposta do sistema, mesmo com o aumento gradual de usuários.
- Possui um modelo otimizado de componentes, possibilitando a criação de interfaces dinâmicas sem comprometer o desempenho do sistema.
- Com o React, apenas os componentes visualizados no momento é que são renderizados, o que diminui o uso de recursos do processador e mantém o sistema com bom desempenho.
- O React recebe atualizações frequentes de modo a corrigir vulnerabilidades e sempre reforçando a sua segurança.
- Os componentes do React são reutilizáveis, o que reduz o tempo de desenvolvimento, de correções e demais alterações.
- Ele provê uma vasta quantidade de recursos de UI para a construção de interfaces com boa estética e responsividade. Além de recursos sólidos para construção de formulários, questionários, dashboards e incorporação de vídeos, que teremos em nosso sistema.

- A arquitetura modular torna a aplicação mais escalável e as alterações são realizadas mais rapidamente.

Back-end

Node.js com Express

- Não é necessário utilizar outra linguagem além do JavaScript, pois o Node.js, assim como o React também se baseia nela.
- O Express possibilita a construção rápida de API RESTful e API Gateway.
- São tecnologias com boa escalabilidade.
- Provê e mantém o bom desempenho com requisições assíncronas, com loops de eventos eficientes.
- Suporte nativo para arquivos JSON para troca de dados entre a Aplicação e o Cliente, de modo eficiente.

Banco de dados

MySQL

- O MySQL tem suporte a consultas SQL mais complexas, é uma tecnologia madura e confiável e possibilita registrar todas as operações feitas na base de dados. Isso facilita a investigação de problemas bem como auditoria.
- Possui interface intuitiva e diversos recursos pertinentes.

Servidor de Aplicação

DigitalOcean

- Interface amigável.
- Plano gratuito que possibilita até 1GB de transferência de dados, HTTPS automático e deploy a partir do GitHub.
- Tem suporte para armazenamento temporário de registros de eventos.

Servidor de Banco de Dados

DigitalOcean

- Permite o uso e provê suporte ao MySQL e 2GB de armazenamento no trial.
- Suporte personalizado sem custo.

Roadmap

O roadmap foi criado para guiar as principais etapas e entregas do projeto, garantindo um desenvolvimento estruturado e transparente. Ele oferece uma visão clara das fases e prioridades do projeto, alinhando os esforços da equipe com os objetivos de negócios e as necessidades dos clientes. Com o roadmap, pretendemos assegurar que cada etapa seja executada de forma coordenada e eficiente.

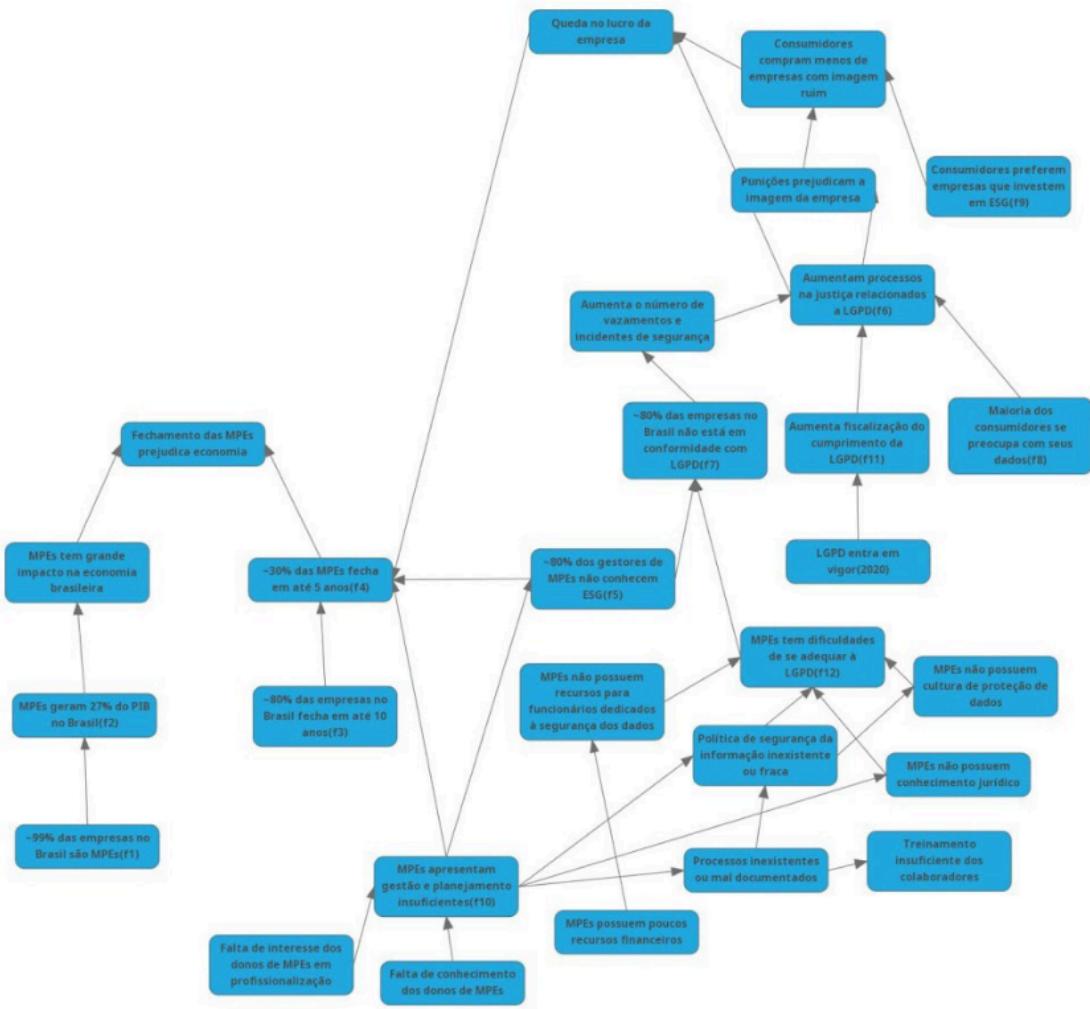
Roadmap



Link: [Roadmap](#)

1. Planejamento (2 semanas)

Foram realizadas discussões para estruturar o problema principal — a dificuldade de adequação de pequenas empresas à LGPD — e definir seu escopo. Também se debateu o objetivo real da proposta de solução. Para auxiliar nesse processo, foram utilizados artefatos como SODA e Canvas de Hipótese.



Link: [SODA](#)

O SODA nos trouxe indicadores que mostram algumas dificuldades enfrentadas pelas MPEs, incluindo a falta de políticas e culturas para a proteção de dados de seus clientes. Esses indicadores serviram como ponto de partida para as pesquisas, revelando os principais motivos pelos quais esse tipo de empresa não alcançava um patamar satisfatório em relação à proteção de dados pessoais.

Foram levantados os principais desafios encontrados, que são: a complexidade das medidas relacionadas à legislação e o volume de trabalho necessário, a falta de conhecimento técnico, e o pouco tempo disponível para se dedicar ao conhecimento necessário.

A partir disso, foi elaborado o Canvas de Hipótese de Negócio com o objetivo de criar uma proposta de solução que tornasse o processo de adequação mais fácil, reduzindo ou amenizando os desafios apresentados anteriormente. Os resultados esperados com essa

solução eram que ela fosse de fácil uso, com baixo custo e que não demandasse muito tempo de quem estivesse responsável pelo processo de adequação.

A própria solução deveria conter tudo o que fosse necessário para que, principalmente, pequenas empresas pudessem dar o primeiro passo no caminho da adequação, sem necessidade de nenhum investimento inicial, como consultorias ou softwares pagos.

2. Análise de requisitos (1 semana)

A partir das primeiras discussões, cada integrante do time se dedicou a aprofundar a compreensão dos requisitos principais da solução, das necessidades e dores dos clientes, e das soluções existentes, bem como das possíveis melhorias. Este processo envolveu uma série de atividades investigativas e analíticas para garantir uma abordagem bem fundamentada e direcionada.

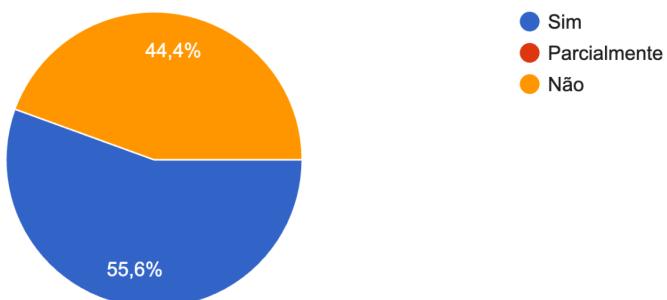
Primeiramente, foram realizadas reuniões com gestores de pequenas e médias empresas (MPEs) para obter insights diretos sobre os desafios enfrentados na adequação à LGPD. Estas conversas forneceram uma visão prática e realista das dificuldades e das expectativas dos usuários finais. Além disso, a equipe conduziu uma extensa pesquisa em artigos acadêmicos, revistas especializadas e guias práticos, que ajudaram a embasar teoricamente a nossa abordagem e a identificar boas práticas e tendências emergentes no campo da proteção de dados.

Como parte da análise de requisitos e levantamento de informações sobre a solução, foi elaborado um formulário (Nível de Conformidade e Percepção da LGPD na visão das Empresas) para entender a percepção de algumas empresas sobre a LGPD e o processo de adequação. O principal objetivo era identificar organizações interessadas no tema que poderiam colaborar no desenvolvimento da proposta de solução.

GRÁFICO 5 – Percentual de empresas que estão em conformidade com a LGPD

A sua empresa está em conformidade com a LGPD?

9 respostas

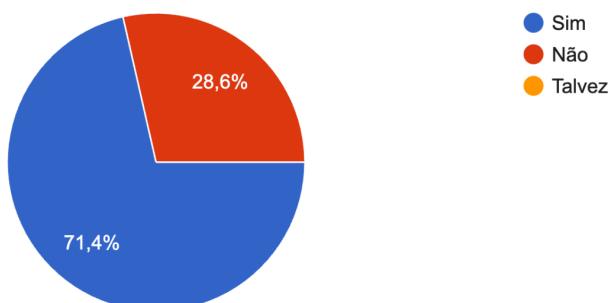


Fonte: Elaborado pelo autor

GRÁFICO 6 – Percentual de empresas que manifestaram interesse em participar do projeto

A empresa tem interesse em participar do desenvolvimento de um sistema que auxilia empresas a se adequarem à LGPD?

7 respostas



Fonte: Elaborado pelo autor

3. Design (2 semanas)

Esta etapa envolveu modelar os processos e definir a estrutura e o design da solução. Para isso, utilizamos artefatos como PM Canvas, PBB, Storyboard e a ferramenta Figma, que exemplificam a interação do usuário de forma clara e intuitiva.

Outros artefatos essenciais para esclarecer a ideia do projeto, foram os Mapas Conceitual e Mental. O Mapa Conceitual abordou os conceitos chave e os domínios de negócio envolvidos no problema escolhido. Ele destacou pontos críticos que exigem atenção, como recursos necessários, complexidade legal, falta de clareza sobre gargalos,

processos internos da empresa e gerenciamento de dados. Já o Mapa Mental foi utilizado para delinear a solução de forma geral, abordando seus objetivos, benefícios, funcionalidades, tipos de usuário e impactos esperados.

4. Desenvolvimento (8 semanas)

Nesta fase, serão implementadas as funcionalidades principais da solução, são elas:

- Cadastro da empresa - Permite o registro detalhado de informações sobre as empresas que utilizarão o sistema, incluindo dados corporativos, contatos principais e áreas de atuação. Para facilitar a gestão e a organização das informações das empresas, possibilitando uma personalização da experiência de autodiagnóstico e garantindo que cada empresa receba uma avaliação precisa de acordo com seu perfil.
- Aba Formulário de Autodiagnóstico - Fornece um formulário estruturado com perguntas categorizadas por pilares da LGPD, que devem ser respondidas pelo responsável da adequação da empresa. O formulário garante uma avaliação abrangente e detalhada da conformidade da empresa, abordando todos os aspectos críticos da LGPD.
- Visualização de Etapas Pendentes e Realizadas - Permite que o responsável acompanhe o progresso do processo de aumento do nível de conformidade com a LGPD, identificando as etapas concluídas e pendentes. Isso facilita a gestão do tempo e dos recursos, assegurando a conclusão eficiente de todas as etapas necessárias.
- Visualização de Resultados com Sugestões de Materiais e Ferramentas - Após a conclusão do autodiagnóstico, os resultados são apresentados juntamente com sugestões de materiais de referência e ferramentas que podem ajudar a empresa a melhorar sua conformidade com a LGPD. Fornecendo recursos práticos para a empresa implementar melhorias e acelerar o processo de conformidade.
- Aba de acesso a Cursos - Para ajudar a capacitar a equipe da empresa, promovendo uma cultura de conformidade e assegurando que todos os colaboradores estejam alinhados com as exigências legais, teremos uma funcionalidade para acessar cursos e treinamentos sobre a LGPD.
- Dashboard - Fornece um painel de controle intuitivo e visual, onde o responsável pode acompanhar métricas chave, visualizar o status geral da conformidade e acessar relatórios detalhados. Essa funcionalidade facilita a

análise e a tomada de decisões estratégicas, proporcionando uma visão clara e abrangente da situação da empresa em relação à LGPD.

- **Suporte** - Disponibiliza um canal de suporte técnico e consultivo para auxiliar os usuários em qualquer dúvida ou problema que possam enfrentar durante o uso do sistema.

5. Testes (2 semanas)

Nesta fase, as funcionalidades principais implementadas serão testadas e validadas novamente com o cliente e também com profissionais especializados. Além disso, é crucial re-validar essas funcionalidades com especialistas na legislação da LGPD, incluindo um Data Protection Officer (DPO), sempre que possível.

6. Implantação (4 semanas)

Esta fase é dedicada ao lançamento da solução e ao treinamento dos primeiros clientes pela equipe responsável pela implantação. Além do treinamento, a equipe fornecerá suporte inicial 24 horas para garantir o uso eficiente da solução.

Conforme mencionado anteriormente, o projeto já conta com o interesse de cinco empresas e a colaboração de um profissional técnico do Sebrae. Adicionalmente, estamos preparando materiais de apoio, como manuais e tutoriais, para facilitar a adaptação dos usuários à nova solução. O contato feito anteriormente com o Sebrae será muito útil neste momento, viabilizando um maior alcance da solução. Também serão coletados feedbacks dos primeiros usuários para identificar possíveis melhorias e ajustes necessários antes de uma implementação mais ampla.

7. Pós-Implantação

Esta fase final é dedicada à avaliação contínua e à melhoria constante da solução. A legislação, os requisitos e os conceitos sobre a LGPD devem ser continuamente monitorados para garantir que as atualizações do sistema sejam implementadas o mais rapidamente possível.

Durante essa fase, a equipe responsável realizará avaliações periódicas de desempenho e usabilidade, coletando feedback dos usuários para identificar áreas que necessitam de melhorias.

Além disso, serão conduzidas auditorias regulares para assegurar que a solução permaneça em conformidade com os padrões legais e de segurança.

Itens de desenvolvimento para versões futuras

- Integrar suporte à inteligência artificial para oferecer respostas mais humanizadas e personalizadas, melhorar a eficiência no atendimento ao cliente, reduzir tempos de espera, e fornecer soluções proativas baseadas em análise de dados
- Disponibilizar uma funcionalidade para avaliar e comprovar a adequação dos processos à LGPD
- Fornecer um certificado de conformidade para empresas que responderam o formulário de autodiagnóstico e chegaram ao nível máximo de conformidade
- Disponibilizar questionários para os colaboradores após a conclusão de cada curso, com o objetivo de reforçar o conteúdo aprendido.
- Evoluir os cursos para um sistema de pontuação pode garantir um engajamento mais assíduo dos colaboradores e também promover uma cultura de aprendizado contínuo.

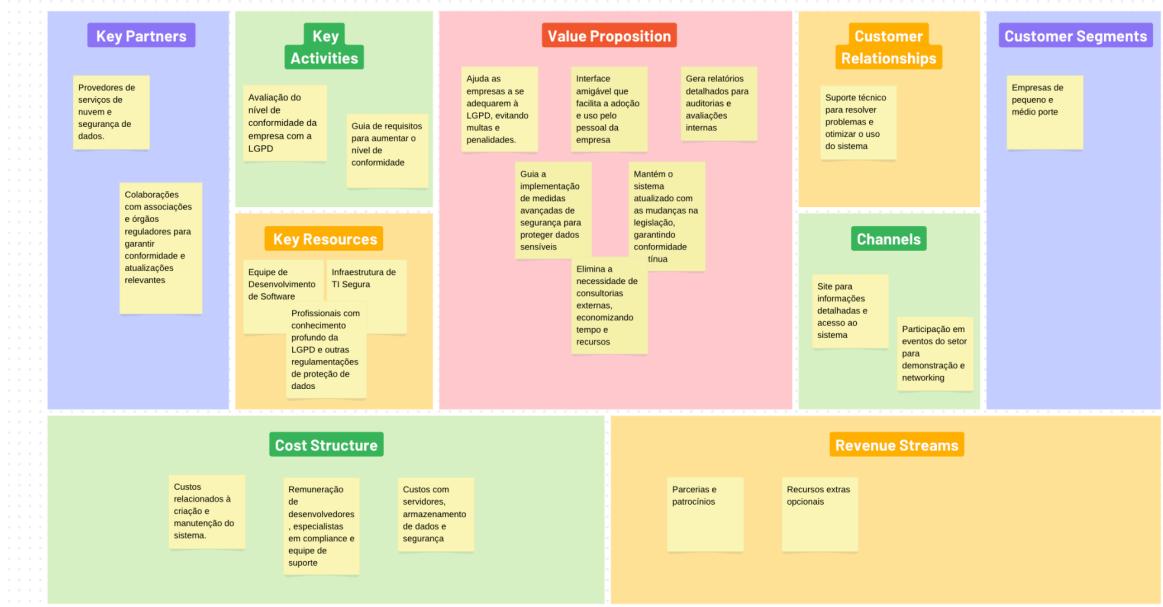
Arquitetura de negócio

Business Model Canvas

O Business Model Canvas (BMC) nos permitiu estruturar de forma clara os principais pontos do modelo de negócio, definindo as relações com os stakeholders, os insumos necessários e os processos vinculados ao plano de negócios. Esta ferramenta facilitou a visualização integrada de todos os componentes essenciais, proporcionando uma compreensão abrangente das interações e dependências que sustentam nosso modelo de negócio.

Link: [Business Model Canvas](#)

Business Model Canvas



Canvas de Hipótese

O Canvas de Hipótese de Negócio, nos permite identificar claramente nossos diferenciais competitivos e compreender profundamente as dores e necessidades do nosso público-alvo. Através desse processo, conseguimos mapear as hipóteses críticas sobre nosso mercado, validar suposições fundamentais e ajustar nossa proposta de valor para atender de maneira mais eficaz às demandas dos clientes.

Link: [Canvas de hipótese de negócio](#)

CANVAS DE HIPÓTESE DE NEGÓCIO		Criador: Data: 09/04/2024	Versão:
<u>TEMA DA MINHA HIPÓTESE</u> Desafios da Implementação da Lei Geral de Proteção de Dados Pessoais (LGPD).		<u>QUEM POSSUI ESSE PROBLEMA?</u> Micro e pequenas empresas principalmente.	
<u>SOLUÇÕES EXISTENTES</u> - Consultorias para a implementação da LGPD nos processos internos das organizações - Ferramentas que auxiliam nas etapas de implementação da LGPD, como gestão de solicitações de titulares, termos de consentimento e geração de relatórios de auditoria.	<u>DORES E SOFRIMENTOS</u> - Desconhecimento sobre os requisitos específicos da LGPD, dificultando a implementação eficaz da conformidade. - Receio em sofrer penalidades em caso de não conformidade. - Custo elevado associado a conformidade com a Lei. - Dificuldade em adaptar processos e sistemas à LGPD.	<u>ATRIBUTOS DA MINHA SOLUÇÃO</u> - Tornar mais prático e simples o acesso às informações de requisitos envolvendo a LGPD para aquele ramo de negócio específico do usuário, facilitando assim a adaptação dos processos internos.	
<u>ANALOGIA DO PROBLEMA / SOLUÇÃO</u> 1º Analogia / Solução: Assim como um guia de trilha mostra o caminho correto a solução envolve, baseado nos dados iniciais inseridos pelo Dono do negócio, expor de forma estruturada como os processos internos da empresa devem ser remodelados ou reestruturados de modo a seguir mais fielmente os princípios e requisitos da LGPD. 2º Analogia / Solução: O governo brasileiro poderia desenvolver uma central ou plataforma integrada para assumir a responsabilidade em relação aos requisitos da LGPD. Com isso, as empresas de todos os portes poderiam terceirizar esse processo, integrando-se ao sistema governamental para autenticação e registro de informações sensíveis. Dessa forma, o governo centralizaria esses dados em sua base, e as empresas/funcionários precisariam solicitar acesso autenticado via reconhecimento facial ou biometria, utilizando o próprio cadastro governamental. Isso geraria históricos de acesso e garantiria a proteção das informações.		<u>POR QUE MINHA SOLUÇÃO É A MELHOR E/OU ÚNICA?</u> - Comparada a uma equipe especializada de segurança de dados, a ideia é que essa solução não custe muito tempo e nem dinheiro. - A solução não deve exigir consultorias externas a equipes especializadas, os próprios membros internos e gestores a partir de inputs no sistema devem conseguir obter resultados satisfatórios.	

Análise SWOT

Através da análise SWOT, podemos avaliar de forma abrangente o ambiente interno e externo, identificando os pontos fortes (Strengths), pontos fracos (Weaknesses), oportunidades (Opportunities) e ameaças (Threats) do projeto. Essa avaliação permite desenvolver estratégias direcionadas para maximizar as forças, explorar as oportunidades, minimizar os impactos das fraquezas e mitigar as ameaças externas.

Link: [SWOT](#)

S	W	O	T
Strengths	Weaknesses	Opportunities	Threats
<ul style="list-style-type: none"> Aumento da conformidade legal; Reducir custos e tempo no processo de adequação a LGPD Facilidade de uso, permitindo a empresa de forma independente realizar as etapas de adequação Materiais acessíveis sobre o tema 	<ul style="list-style-type: none"> Pode não atender perfeitamente a todas as necessidades específicas de diferentes empresas. Dependência de tecnologia, pode ser vulnerável a falhas técnicas 	<ul style="list-style-type: none"> Grande potencial de crescimento à medida que mais empresas buscam conformidade com a LGPD Parcerias estratégicas que podem aumentar a adoção do sistema Oportunidade para integrar novas tecnologias, como IA e machine learning, para melhorar a eficácia do sistema. 	<ul style="list-style-type: none"> Outras empresas podem oferecer soluções semelhantes Alterações na LGPD ou em outras regulamentações de privacidade podem exigir adaptações contínuas no sistema Funcionários podem resistir à mudança

Project Model Canvas

O Project Model Canvas foi montado para adquirir uma visão mais clara sobre o projeto proposto, identificando seus principais aspectos. Com ele definimos o objetivo da solução, seus benefícios e requisitos, além de identificar os principais riscos e restrições que poderiam interferir no seu andamento.

Link: [Project Model Canvas](#)

JUSTIFICATIVAS Passado	PRODUTO	STAKEHOLDERS EXTERNOS & Fatores externos	PREMISSAS	RISCOS
 <ul style="list-style-type: none"> Adequar a organização a a legislação Consumidores preocupados com a proteção de seus dados 	 <p>Um sistema de informação que facilite a adequação das pequenas empresas a LGPD</p>	 <ul style="list-style-type: none"> -Gestores executivos de pequenas empresas - Responsável pelo setor de TI da empresa (caso tenha). - Colaboradores - Clientes - Parceiros comerciais 	 <ul style="list-style-type: none"> Cientes/empresas que atuam com dados pessoais e sensíveis 	 <ul style="list-style-type: none"> Falta de engajamento dos colaboradores Resistência às modificações nos processos
OBJ SMART	REQUISITOS	EQUIPE	GRUPO DE ENTREGAS	LINHA DO TEMPO
 <p>Facilitar o processo de adequação de uma organização à LGPD.</p>	 <ul style="list-style-type: none"> O sistema deverá se apresentar adequado aos diversos ramos empresariais Deve possibilitar a gestão e acompanhamento do processo de adequação a LGPD O sistema estará sempre atualizado com as modificações referentes a LGPD Irá avaliar o nível de conformidade da empresa com a LGPD 	 <ul style="list-style-type: none"> Consultores Analista de processos Consultor Jurídico Desenvolvedores Gerente de projeto 	 <ol style="list-style-type: none"> 1 -Levantamento de processos e requisitos que precisam ser adequados para empresa aumentar seu nível de conformidade 2 - Planejamento para adequação dos processos 3 -Atualização dos instrumentos jurídicos e adoção de tecnologias necessárias para a correta gestão de dados 4 -Conscientização dos colaboradores 	
BENEFÍCIOS Futuro		RESTRIÇÕES		CUSTOS
 <ul style="list-style-type: none"> Maior confiança dos clientes e usuários Redução de riscos e penalidades Aumento da gestão operacional de dados de forma segura Maior valor de mercado 		 <ul style="list-style-type: none"> Recursos limitados 		 <ul style="list-style-type: none"> Tempo mínimo para implementação

Storyboard

Através do Project Model Canvas é possível construir uma visão mais clara sobre o público-alvo da solução proposta, sobre os problemas enfrentados por essas pessoas e sobre as características desejáveis do produto a ser desenvolvido. Para ilustrar de forma mais direta a proposta de valor do SIA LGPD, foi criado o storyboard mostrado a seguir. Foi feito um esforço para descrever de forma lúdica a jornada do usuário desde a descoberta do SIA, passando pelo seu uso e terminando com os benefícios que podem ser obtidos.

Definir a jornada do usuário através de um storyboard proporciona pelo menos três benefícios: direciona o processo de desenvolvimento de software, cria uma forma simplificada de comunicação com potenciais investidores e cria também outra forma de comunicação com potenciais usuários do SIA.

Link: [Storyboard](#)

Storyboard SIA - Sistema Interativo de Autodiagnóstico



Planejamento da POC

O planejamento da prova de conceito foi utilizado com o objetivo de validar a viabilidade do projeto, os passos para execução, os custos previstos, resultados esperados,

etc. Através dessa ferramenta conseguimos comprovar a eficácia e alinhamento da solução com os objetivos e expectativas definidos.

Link: [Planejamento da prova de conceito](#)

Planejamento da Prova de Conceito	
Título da PoC: Formulário de auto-diagnóstico que auxilia na conformidade com a LGPD.	
<p>1. Desafio Concordância das medidas e volume de trabalho necessário para implantação da LGPD.</p> <p>Falta de conhecimento técnico suficiente sobre a LGPD.</p> <p>Pouco tempo disponível para dedicar ao conhecimento, aplicação e adequação à lei.</p> <p>Os participantes devem corrigir as principais deficiências das organizações no momento de implantar as requisições específicas de legislação, que exigem muitas revisões e avaliação de políticas de privacidade, a implementação de medidas de segurança de dados, a realização de avaliações de impacto à privacidade, a análise dos processos internos a meio operações, entre outros.</p>	<p>2. Indicadores Nível de comprometimento da empresa sobre a LGPD - evolução do nível de conhecimento antes e depois do uso do SIA.</p> <p>Nível de conformidade da empresa com a LGPD - evolução do nível de conformidade antes e depois do uso do SIA.</p> <p>Tempo para adequação da empresa à LGPD - comparação com outras empresas.</p> <p>Complexidade durante implementação - quantidade e tipo das dificuldades relatadas pelas participantes.</p> <p>Grau de satisfação dos usuários - nota atribuída à satisfação durante o uso do SIA.</p>
<p>3. Solução O formulário de Auto-diagnóstico (PoC) disponibiliza um formulário que auxilia empresas no desarmazenado do nível de conformidade com a LGPD e na implementação das mudanças necessárias para alcançar a adequação.</p> <p>Após o preenchimento do formulário o usuário recebe o nível de conformidade em que se encontra sua organização, assim como dicas para aumentar seu nível, matérias de referência e ferramentas recomendadas.</p> <p>Após a conclusão de cada etapa de adequação, o usuário pode avaliar a eficiência da ferramenta de adequação e fornecer feedbacks e sugestões.</p>	<p>4. Resultados Maior clínica sobre a importância da LGPD para pelo menos 100 empresas.</p> <p>Definição do nível de adequação à LGPD para pelo menos 20 empresas.</p> <p>Implementação de medidas de adequação para pelo menos 10 empresas.</p> <p>Aumento do nível de adequação para pelo menos 5 empresas.</p> <p>Menor exposição à incerteza de mudanças e processos.</p> <p>Diminuição de riscos de decisões.</p> <p>Maior competitividade com o mercado global.</p> <p>Maior proteção de transparéncia e confiança.</p> <p>Promover inovação responsável.</p>
<p>5. Hipóteses Aumento do comprometimento das empresas sobre a implementação da LGPD - evolução da eficácia da conformidade.</p> <p>Níveis de conformidade da empresa com a LGPD - evolução do nível de conformidade antes e depois do uso do SIA.</p> <p>Tempo para adequação da empresa à LGPD - comparação com outras empresas.</p> <p>Complexidade durante implementação - quantidade e tipo das dificuldades relatadas pelas participantes.</p> <p>Grau de satisfação dos usuários - nota atribuída à satisfação durante o uso do SIA.</p>	<p>6. Equipes Número parte das empresas de pequeno porte, o dono.</p> <p>Em algumas, um funcionário vai acumular a responsabilidade pela adequação.</p> <p>Em poucos casos existem pressos ou departamentos encarregados de TI.</p>
<p>7. Recomendado Mais comprometimento dos participantes - desistência, demora no uso, exemplo, demora na comunicação.</p> <p>Enforcement das operações de uso ou mais participantes.</p> <p>Necessidade de adequações extras e demandas - adição de melhorias.</p> <p>Preenchimento incorreto do formulário e SIA.</p> <p>Mutuas na LGPD.</p> <p>Incapacidade do time - desinteresse, dores, imprevisões.</p> <p>Indisponibilidade de recursos tecnológicos - Site, links, e-mail, chat, etc.</p>	<p>8. Orientações Promover o uso de ferramentas gratuitas do Google Docs para elaboração dos questionários e criação dos relatórios - custo R\$0 - princípio inicial.</p> <p>Uso de meios de comunicação conversacional-mal, chat, etc), necessários para alcançar maior contato com as participantes - custo R\$0.</p> <p>Futuramente criação do MVP baseado em aplicativo web usando serviços de hospedagem gratuita como Supabase - custo R\$0 - princípio estável.</p>
<p>9. Macroperspectivas Conjunto de perguntas de alto nível para entrevistas de empresas;</p> <p>Questionário para análise de empresas;</p> <p>Relatório de consulta com especialistas;</p> <p>Lista de empresas para acompanhamento prático;</p> <p>Lista de empresas para acompanhamento geral;</p> <p>Relatório de entrevistas;</p> <p>Relatório do questionário de análise;</p> <p>Protocolo simplificado;</p> <p>Análise das respostas ao protocolo simplificado;</p> <p>MVP - Produto Minimo Viable;</p>	<p>10. Linha de Tempo Sprint1. Levantamento e edição de materiais sobre a LGPD para estruturação do questionário de análise de empresas e o questionário de entrevista.</p> <p>1.1. Questionário de desenvolvimento, inicia as fases de descrição de clientes e validação dos critérios de classificação das empresas para o levantamento de entrevistas.</p> <p>Sprint2. Conjunto de empresas selecionadas, realizar a aplicação do questionário em alto nível para adquirir mais informações e validar os critérios de classificação.</p> <p>2.1. Análise de respostas do questionário de alto nível e validação das classificações.</p> <p>Sprint3. 3.1. Elaboração de protocolo simplificado, com o uso de um software de gerenciamento de projetos para a execução das adequações necessárias no questionário de entrevista.</p> <p>Sprint4. Iniciar fase de validação do protocolo com as empresas.</p> <p>4.1. Realizar os refinamentos necessários de acordo com as respostas.</p> <p>Sprint5. 5.1. Criar MVP e aplicá-lo de forma prática nas empresas e receber feedbacks para aprimorar a estruturação e aplicação.</p> <p>Sprint6. 5.1. Análise das respostas do MVP e questões.</p> <p>Sprint7. 6.1. Elaborar o Experimento Base para a estruturação e validação do formulário.</p> <p>6.1. Revisar todos os documentos elaborados desde a Sprint 1, testando as interações e ajustando os materiais.</p>
<p>11. Stakeholders Globais envolvidos em pequenas organizações.</p> <p>Responsável pelo setor de informação da empresa (TI); caso tenha.</p> <p>Clínicas das empresas.</p> <p>Funcionários em geral.</p> <p>Professor especialista em segurança de dados (ofertado externo).</p> <p>Professora de consultoria (ofertado externo).</p>	<p>12. Implementação PoC Início da fase de desenvolvimento de software para a entrega da primeira versão completa do sistema.</p> <p>Uso do modelo Running Lean, com suas principais e ferramentas (como Lean Canvas) para criação e evolução do desenvolvimento do produto (software).</p> <p>Busca de financiamento.</p>

Product Market Fit

Para avaliar se o projeto atende às necessidades e desejos do mercado, elaboramos a análise de Product-Market Fit. Essa ferramenta nos permite obter uma nova perspectiva sobre a interação entre produto, cliente e mercado, ajudando a identificar as métricas mais importantes para o desenvolvimento do produto e analisar o quanto ele satisfaz as necessidades dos clientes.

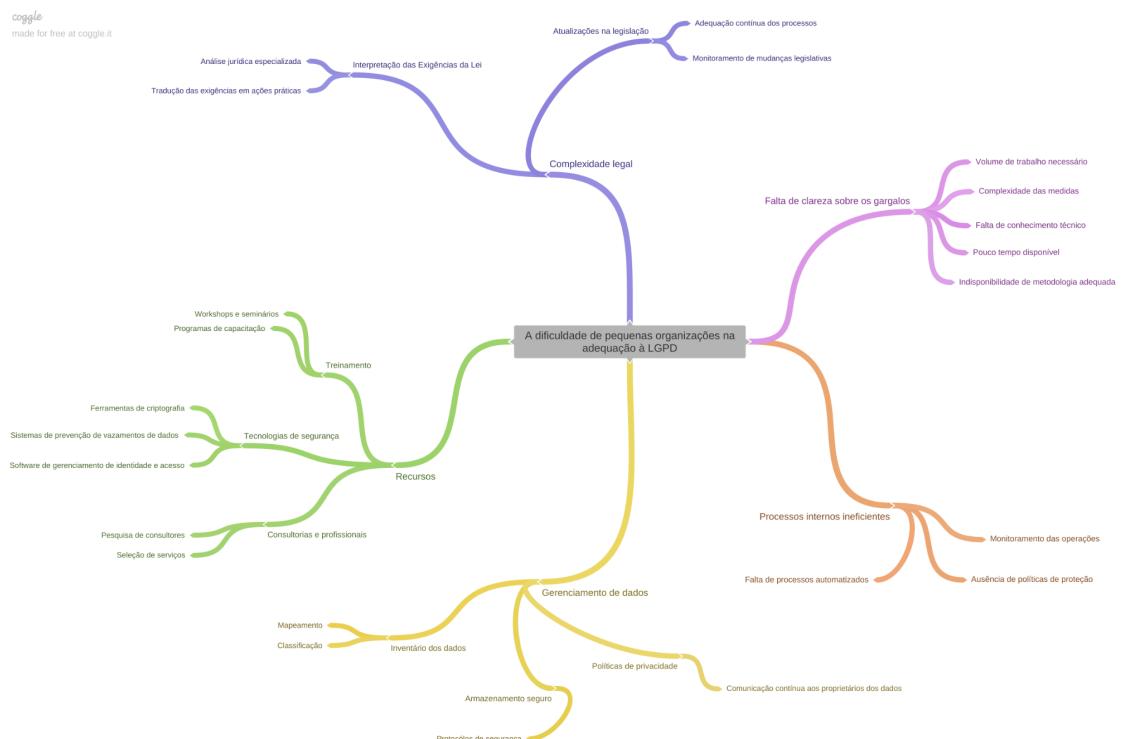
Link: Product Market Fit

Customer		Product
Characteristics and jobs to be done	<>	Alternatives
Empresas de pequeno e médio porte		Serviços de treinamento e capacitação Serviços de Consultoria
Problems and needs	<>	Key features
Risco de multas e penalidades por não conformidade		Formulário de autodiagnóstico para avaliação do nível de conformidade da empresa
Dificuldade em entender e implementar todas as exigências da LGPD		Etapas para aumentar o nível de conformidade da empresa com a LGPD
Falta de recursos internos para gerenciar a conformidade de maneira eficaz		
Channel	<>	Value for the channel
Site para informações detalhadas e acesso ao sistema		Redução de riscos e penalidades Maior valor de mercado Maior confiança dos clientes e usuários
User experience	<>	Key metrics
Organização busca se adequar a legislação		Pesquisa de satisfação ao concluir cada etapa de adequação Evolução do nível de conformidade antes e depois do uso do SIA Complexidade durante implantação: quantidade e tipo das dificuldades relatadas pelas participantes
Responsável procura garantir maior proteção para os dados utilizados nos processos		
Responsável acessa o SIA para avaliar o nível de conformidade da empresa		

Mapa conceitual

Para compreender e estudar os impactos causados pelo problema "A dificuldade de pequenas organizações na adequação à LGPD", elaboramos um mapa conceitual. Esse mapa estrutura e organiza as informações de maneira clara e lógica, facilitando a análise e a visualização das principais questões envolvidas.

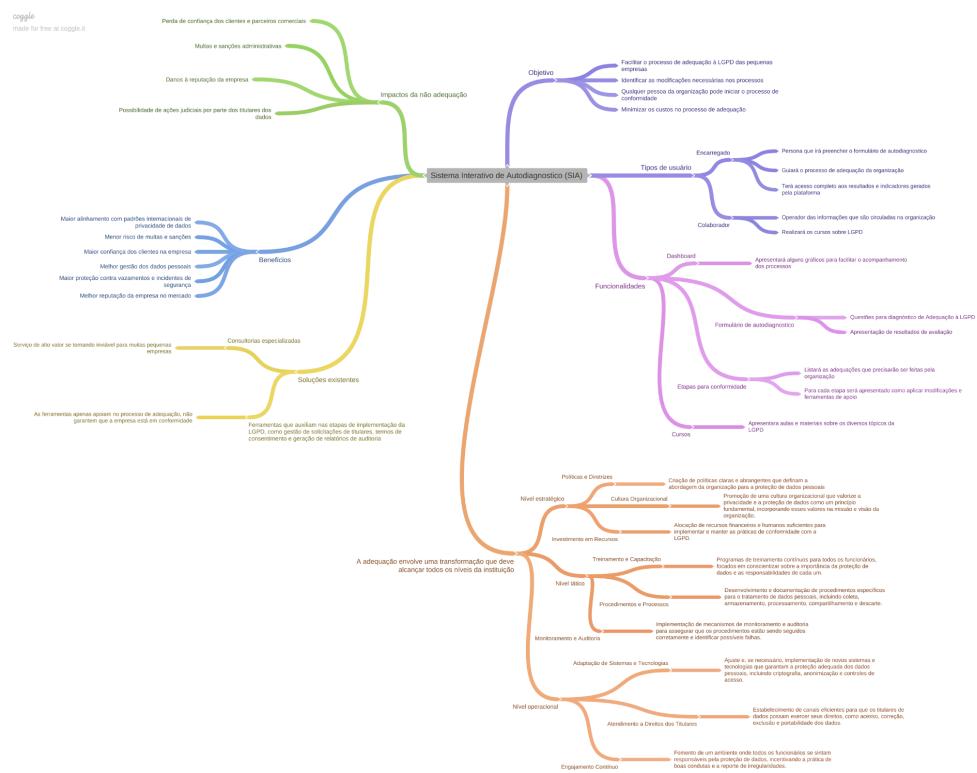
Link: [Mapa Conceitual](#)



Mapa Mental

Utilizamos o mapa mental para ilustrar a análise completa do Sistema Interativo de Autodiagnóstico (SIA), mapeando impactos gerados, seus objetivos, funcionalidades e personas.

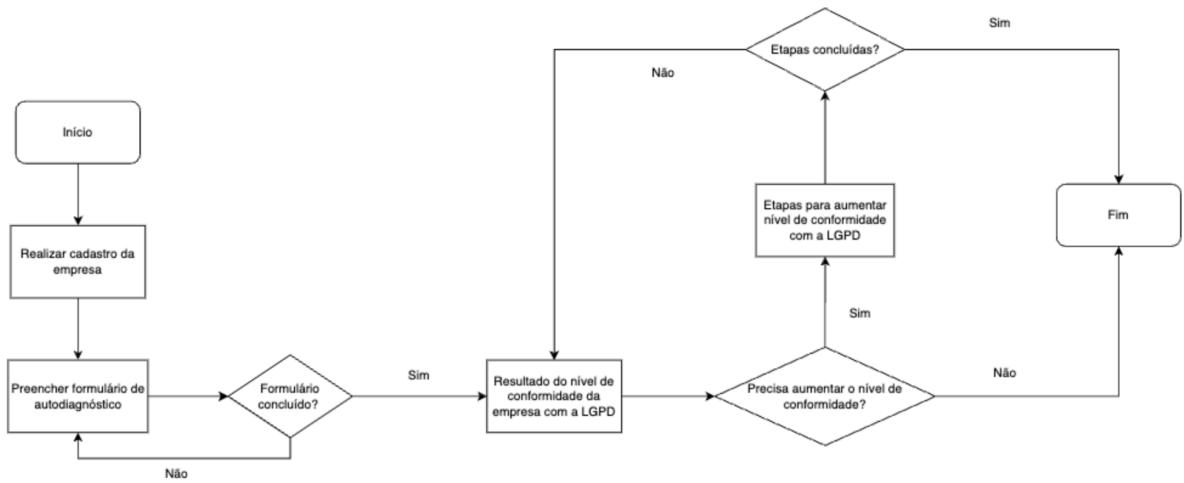
Link: [Mapa Mental](#)



Business Process Model and Notation

Para representar visualmente o processo de aplicação, utilizamos o Business Process Model and Notation (BPMN). Esta notação nos permite mapear detalhadamente o fluxo do processo, desde o seu início até o término, incluindo todas as suas variantes e possibilidades.

Link: [BPMN](#)



Guia de etapas para nível de maturidade

De acordo com o escopo do projeto, com base nas respostas do formulário de autodiagnóstico, a empresa recebe uma avaliação detalhada do seu nível de conformidade atual. Os resultados indicam o grau de conformidade alcançado e destacam as áreas que necessitam de melhorias para aumentar esse nível.

Essa representação visual serve como um guia prático para que a empresa entenda suas atuais deficiências e saiba exatamente quais passos tomar para alcançar uma maior conformidade, promovendo uma gestão mais eficiente e alinhada aos padrões estabelecidos na LGPD.

A ideia de níveis de maturidade e as dimensões se baseiam na Tabela de Atributos de Maturidade do CobiT 4.1, por ser um modelo com propósitos semelhantes aos do SIA.

A principal referência para a definição das etapas de adequação foi o Manual Prático De Adequação À Lei Geral de Proteção de Dados para Micro e Pequenas Empresas do IDEC mas também foram relevantes a cartilha Simplificando a LGPD nos Negócios do Sebrae além do Guia Orientativo Segurança Da Informação Para Agentes De Tratamento De Pequeno Porte da ANPD.

Link: [Etapas nível de maturidade](#)

Etapas nível de maturidade

	Cultura de Proteção de Dados	Processos	Ferramentas	Habilidades	Responsabilidade
5	Esse treinamento ocorre periodicamente com atualizações sobre novas práticas.	Deve-se definir indicadores para monitorar a melhoria contínua no fluxo dos processos.	Defina uma pessoa encarregada pelos dados, as ferramentas devem ser revisadas e atualizadas periodicamente.	A equipe encarregada deve analisar e aprimorar continuamente o fluxo de dados, política de segurança e termos de uso.	Deve-se nomear a Pessoa Encarregada de Dados, ele será responsável pela segurança dos dados na organização e pela equipe de segurança.
4	Todos os colaboradores e gestores da empresa deverão ter passado por treinamento e já entendem as boas práticas relacionadas a proteção de dados.	Deve-se monitorar e documentar todo acesso feito, com um histórico de logs do que foi acessado e o horário.	A empresa deve possuir a documentação completa da política de segurança existente e dos termos de uso do negócio, bem como demonstrar que é aplicado diariamente.	Definir uma equipe para analisar e melhorar os fluxos de dados existentes e também para formular, atualizar e aplicar a política de segurança e termos de uso referente a manipulação de dados.	A partir da criação de controles de acesso e segmentação de permissões deve-se estabelecer os responsáveis pela segurança dos dados em cada momento do fluxo de operação.
3	Investir em materiais de conscientização e treinamentos sobre a proteção de dados.	Definir acessos controlados para cada operação/processo existente na empresa, identificando essa pessoa.	Deve-se mapear o fluxo dos dados que a empresa控制a e criar uma política e termo de uso para a manipulação desses dados.	Encarregar um ou mais colaboradores com a função de mapear/atualizar o fluxo de dados, bem como atualizar as políticas e termos de uso.	Deve estar definido que em último caso, os donos da empresa são responsáveis pela segurança dos dados manipulados.
2	Incentivar o diálogo entre funcionários para aumentar a discussão do assunto na empresa.	Definir ao menos um processo que controle o acesso e manipulação dos dados.	A empresa deve fazer o controle de dados usando algum meio, mesmo que informal.	Todos os colaboradores devem ser capazes de usar algum mecanismo informal de controle de dados.	Informalmente, a pessoa responsável pela manipulação de um conjunto de dados é responsável pela sua segurança.
1	Pelo menos um funcionário na organização discute a proteção das informações que a empresa controla.	Nesta etapa não é exigido um processo formal que declara como é feita a manipulação dos dados.	Nesta etapa não é exigido que a empresa controla os dados com alguma ferramenta.	Nesta etapa não é exigido que os colaboradores possuem um grau de habilidade mínima ou que exista um programa de treinamento para manipulação de dados.	Nesta etapa não é exigido a definição formal de responsabilidades.

Lógica para o cálculo de nível de maturidade

O formulário de autodiagnóstico foi desenvolvido com base em um sistema de pontuação. Cada pergunta é categorizada dentro de um dos pilares de conformidade com a LGPD e possui um peso determinado conforme sua relevância. O objetivo é fornecer uma avaliação precisa e detalhada do nível de conformidade da empresa em relação à LGPD.

Para definir os critérios da pontuação foram usadas como referência a cartilha Simplificando a LGPD nos Negócios do Sebrae e a Ferramenta de Diagnóstico LGPD criada pela Associação Brasileira das Empresas de Software. Na planilha abaixo, detalhamos a categorização de cada pergunta e explicamos como o cálculo das respostas é realizado para definir o nível de conformidade da empresa.

Link: [Lógica de pesos e faixa de pontuações](#)

QUADRO 1 – Pesos de acordo com o grau de importância

Pesos de acordo com grau de importância daquela pergunta para a adequação :	
3	Menos importante
5	-
7	-
8	-
10	-
15	Mais importante

Fonte: Elaborado pelo autor.

QUADRO 2 – Quantidade de pontos por nível de maturidade

Distribuição da faixa de pontos por nível de maturidade baseado nas respostas que o sistema espera que uma organização de determinado nível responda

Nível 1	0-53 pontos
Nível 2	54-94 pontos
Nível 3	95-130 pontos
Nível 4	131-160 pontos
Nível 5	161-171 pontos

Fonte: Elaborado pelo autor.

Análise de Mercado

1. Necessidades e dores dos clientes

A implementação eficaz da conformidade com a LGPD enfrenta diversos desafios. O desconhecimento sobre os requisitos específicos da lei dificulta a aplicação correta das suas diretrizes. Além disso, há um receio generalizado em sofrer penalidades severas em caso de não conformidade, o que gera insegurança entre as empresas. Outro obstáculo significativo é o custo elevado associado à adequação dos processos e sistemas à LGPD, que pode ser oneroso para muitas organizações. A adaptação dos procedimentos e tecnologias existentes para atender às normas estabelecidas pela lei também se mostra desafiadora, exigindo tempo e recursos consideráveis.

2. Análise da concorrência

Atualmente, existem consultorias para a implementação da LGPD nos processos internos das organizações, mas seus custos podem ser proibitivos para pequenas empresas. Além disso, ferramentas que auxiliam na implementação da LGPD, como gestão de solicitações de titulares, termos de consentimento e geração de relatórios de auditoria, também têm preços elevados e muitas vezes não cobrem de forma abrangente todos os processos da empresa, focando apenas em aspectos individuais. Nosso sistema busca suprimir a necessidade de uma equipe especializada de segurança de dados, a ideia é que essa solução não demande muito tempo nem dinheiro. A solução não exigirá consultorias externas ou equipes especializadas; os próprios membros internos e gestores, a partir de inputs no sistema, devem conseguir obter resultados satisfatórios.

Ferramentas e serviços concorrentes	Pontos negativos
Contratação de consultoria especializada	<ul style="list-style-type: none"> a. Custo total estimado de R\$20.000,00 em 2020 b. Daryus, DropReal, GetPrivacy, Sebrae, etc c. Solução inviável para a maioria das MPEs que quer gastar de R\$0 a R\$10.000
Cursos e treinamentos	<ul style="list-style-type: none"> a. Inúmeros pagos e gratuitos b. RD Station (Marketing), Sebrae, Udemy, MANUAL

	<p><u>PRÁTICO DE ADEQUAÇÃO À LGPD - IDEC</u>, etc</p> <ul style="list-style-type: none"> c. Materiais gratuitos são difíceis de encontrar (conhecimento pulverizado) e tem qualidade variável d. Materiais pagos são mais completos e. Exigem investimento de nenhum ou pouco dinheiro mas de tempo significativo
Implantação de sistemas prontos	<ul style="list-style-type: none"> a. <u>Privacy Tools</u>, <u>DPOnet</u>, <u>Meus Dados</u>, <u>LGPDgo</u>, etc b. Custo menor, mas recorrente com assinaturas ou atualizações c. Não elimina necessidade de adequações nos processos d. Ainda exige treinamento e. Necessidade de encontrar sistema adequado à rotina da empresa
Adequação por iniciativa interna da empresa	<ul style="list-style-type: none"> a. É possível que a própria empresa busque as informações e faça as mudanças necessárias b. Investimento enorme de tempo c. Propensão a erros

3. Principais diferenciais

A solução proposta oferece diferenciais significativos ao tornar prática e acessível uma ferramenta que auxilia pequenas organizações a iniciarem suas adaptações à LGPD. O objetivo é permitir que essas empresas deem o primeiro passo na conformidade sem a necessidade de contratar consultorias especializadas, participar de cursos e treinamentos caros, ou investir em softwares com custos elevados e recorrentes. A ideia central é que, através da resolução de um formulário, a organização possa rapidamente avaliar seu nível atual de conformidade (aproximado) e, com base nisso, iniciar as adaptações necessárias utilizando as sugestões fornecidas pela plataforma.

A proposta visa facilitar o acesso à informação sobre os requisitos de adequação à LGPD, unificando diversos materiais em uma única plataforma. Esse processo é

acompanhado por uma validação e apuração das fontes, garantindo a referência mais atualizada possível, analisada por profissionais qualificados.

Nosso objetivo é reduzir o tempo que a organização precisa gastar buscando material e treinando seus profissionais para iniciar o processo de adequação. Nossa solução é projetada para tornar a LGPD mais acessível, prática e econômica, permitindo que pequenas empresas atinjam a conformidade de maneira eficiente e com menor custo.

4. Consulta de especialistas para validação da ideia de negócio

Além de entrevistar potenciais clientes para entender seus problemas e pedir opiniões a respeito do SIA, buscamos a opinião de especialistas. Enviamos mensagens para a Endeavor Brasil, para o Centro de Empreendedorismo e Incubação da Universidade Federal de Goiás e para o Sebrae. Apenas o Sebrae respondeu e tivemos duas interações com eles.

Na primeira interação, com uma especialista em planos de negócios, nos foi dito que existe uma demanda pelo tipo de sistema que propomos e que a necessidade de adequação à LGPD só tende a aumentar junto com a fiscalização e a aplicação de punições. A especialista nos informou que não poderia fornecer apoio imediato, mas que encaminharia nossa solicitação para o setor de inovação.

Na segunda interação, uma analista técnica nos solicitou o envio de um ofício para o Diretor Técnico do Sebrae contendo informações detalhadas sobre o SIA e as formas de apoio pedidas. O ofício é um pedido formal de apoio a longo prazo para o desenvolvimento de um produto pronto para o mercado. Como existe a expectativa de que o produto a ser desenvolvido esteja em um estado mais avançado de maturidade do que o possível dentro do escopo da Residência Técnica, não foi possível formalizar o pedido de apoio. No entanto, consideramos que os recursos do Sebrae serão de grande utilidade para as fases seguintes.

Proposta de Criação de DAO para o SIA LGPD

Nesta seção são descritas as vantagens que podem ser obtidas a partir da criação de uma DAO para gerenciar e manter o SIA LGPD, além das características desejáveis dessa DAO. As possibilidades existentes para os principais atributos de uma DAO são listadas e comparadas e a mais apropriada para o SIA é apontada.

Vantagens e desvantagens da utilização de uma DAO

DAOs permitem que grupos de participantes diversos reúnam capital e força de trabalho para atingir objetivos comuns com transparência e rapidez. A movimentação de recursos financeiros ocorre de forma instantânea sem depender de instituições tradicionais. As decisões são tomadas de acordo com votações registradas em blockchain, seguindo as regras pré-estabelecidas da organização, permitindo a resolução rápida de problemas de

forma democrática e transparente. O aspecto digital e o alto grau de automação tornam o processo de votação mais barato e eliminam a necessidade de várias camadas intermediárias de gerência. A facilidade de influenciar as decisões incentiva participantes minoritários a contribuírem, representando os interesses mais diversos (WRIGHT, 2020) (FÓRUM ECONÔMICO MUNDIAL, 2022).

Apesar dos inúmeros benefícios, o uso de DAOs apresenta riscos relacionados à incerteza regulatória (WRIGHT, 2020) (FÓRUM ECONÔMICO MUNDIAL, 2022), vulnerabilidades (GEORGE, 2024) (FÓRUM ECONÔMICO MUNDIAL, 2022) que podem causar prejuízo financeiro ou dar margem para manipulação de votos, além de precisar de mecanismos de votação bem pensados para garantir representatividade (BARBEREAU, 2023).

Propósito da DAO

Esta DAO será criada para realizar três atividades principais:

1. Realizar o desenvolvimento, operação e manutenção dos sistemas necessários para o funcionamento do SIA LGPD.
2. Organizar as decisões de governança e eleger as entidades responsáveis pela aplicação dessas decisões.
3. Fazer o recebimento, a guarda e a distribuição dos tokens e das moedas fiduciárias da organização. Os tokens e moedas podem ser recebidos de participantes da rede ou financiadores externos e podem ser distribuídos como recompensa por contribuições necessárias à DAO, para custeio de despesas necessárias ou para investimentos.

O problema que a DAO busca resolver é o baixo nível de adequação à LGPD das empresas pequenas no Brasil. Os administradores destas empresas relatam ter interesse em se adequar mas não encontram meios fáceis e/ou baratos de fazê-lo. A falta de boas práticas de proteção a dados expõe os clientes dessas empresas a vazamentos que podem causar prejuízo financeiro, emocional e a integridade física.

Com a criação do SIA, mais empresas podem se adequar à LGPD, consequentemente protegendo melhor a sociedade de fraudes, golpes, extorsão, exposição indevida e assédio. Todos os interessados nessa melhoria podem participar da DAO e contribuir com as melhores práticas de proteção de dados a serem usadas por milhares de empresas.

Atores envolvidos

Os atores presentes em maior quantidade são **empresas em processo de adequação à LGPD ou de melhoria contínua** que recebem algum retorno pelo investimento na compra de tokens. O sistema será criado para servir prioritariamente a estes atores e as operações da DAO devem refletir isso.

Os incentivos para que empresas participem da DAO são primeiramente utilizar o SIA para atingir um nível mínimo de adequação e posteriormente realizar o processo de melhoria contínua de adequação à LGPD. Participando da DAO, essas empresas podem pedir e discutir mudanças no SIA, de modo a aumentar a qualidade do serviço prestado.

Presentes em menor quantidade mas de importância fundamental são os atores responsáveis pelo desenvolvimento, operação e manutenção contínuos do SIA e da DAO. Essas pessoas e entidades precisam manter a qualidade e corrigir falhas do software e da infraestrutura, garantindo a melhor experiência possível para todos os usuários. Além da parte tecnológica, é fundamental que especialistas de domínios como direito, contabilidade e negócios mantenham os conteúdos do SIA atualizados e relevantes para os usuários finais e estejam sempre atentos às críticas e oportunidades de melhoria. Estes **atores responsáveis pela operação e pelos aprimoramentos do SIA** podem ser remunerados com tokens ou opcionalmente com moeda fiduciária caso participem da DAO ou exclusivamente com moeda fiduciária caso não participem.

O incentivo para a participação dos mantenedores é primeiramente financeiro. Para cada contribuição que fizerem serão remunerados com uma quantia acordada pela comunidade. Utilizando a experiência de longa data dos projetos de software livre e aberto, é possível atrair contribuidores que buscam recompensas diferentes das puramente financeiras como reconhecimento diante da sociedade, promoção de uma causa de interesse, resolução de desafios técnicos e aprimoramento de habilidades valorizadas no mercado. Empresas também podem incentivar a contribuição dos seus próprios funcionários de forma remunerada. Para atrair estes contribuidores deve existir um esforço constante de promoção da DAO e de como as atividades de contribuição se alinham com os interesses destes contribuidores.

Outro grupo de atores que pode se interessar pela participação na DAO são **clientes das empresas** que usam o SIA, por serem afetados diretamente pelo sucesso ou fracasso do sistema.

O incentivo para a participação dos clientes é ter um contato mais próximo com as empresas que o interessam. Com essa proximidade é possível questionar e observar quais esforços a empresa faz para proteger seus dados e continuar realizando transações com mais confiança. Os clientes também podem se manifestar, expondo um ponto de vista talvez desconsiderado pelos outros atores, trazendo melhorias para o SIA. Assim os clientes se sentem ouvidos e representados.

Por fim, **órgãos governamentais e acadêmicos** podem consultar os participantes da DAO sobre questões regulatórias e seus impactos, além de fornecer aconselhamento e referências para facilitar o processo de conformidade com a LGPD.

Os órgãos governamentais e acadêmicos têm nesta DAO uma oportunidade valiosa de discutir com antecedência a legislação relacionada à proteção de dados, auxiliar na sua implementação e mensurar os impactos diretamente nas partes mais afetadas, as empresas e os consumidores. Logo, o incentivo para a participação dessas entidades é a comunicação direta com as partes interessadas e o acesso a dados de qualidade para fundamentar políticas públicas e pesquisa.

Considerando que a DAO fará a comercialização de tokens com valor comercial e que estes tokens podem ser negociados livremente entre os participantes da rede, pode existir um incentivo de especulação financeira para a compra e acumulação de tokens por qualquer tipo de ator.

Uma mesma pessoa ou entidade pode se apresentar como múltiplos atores.

Estrutura de governança

É prevista a possibilidade de que **todas as decisões e características da DAO podem mudar totalmente a qualquer momento** através dos mecanismos de votação da própria DAO.

Participantes da DAO devem ser eleitos para ocupar cargos de gestão da DAO e intermediar as interações com organizações tradicionais fora da blockchain. Também devem existir participantes dispostos a realizar tarefas relacionadas à operação contínua da DAO e do SIA, compensados com tokens. Esses participantes podem ser eleitos para cargos fixos ou receber recompensas pela realização de tarefas pontuais.

Frequentemente decisões precisam ser tomadas e para isso deve existir um mecanismo de votação. Qualquer participante pode propor uma consulta que resulta em um simples consenso ou na execução de contratos inteligentes que causam alterações na estrutura da DAO e/ou na alocação de recursos. A consulta será levada a toda a rede caso um número suficiente de participantes demonstre interesse na sua realização.

O **resultado pode ser determinado através da maioria simples**. No entanto, para refletir o propósito da DAO (atender aos interesses das empresas que buscam adequação à LGPD), o voto de cada grupo de atores tem um peso diferente. Em cada consulta, uma **empresa** em adequação tem direito a **oito votos**, um **mantenedor** tem direito a **quatro votos**, um **cliente** tem direito a **dois votos**, um **órgão governamental** ou **acadêmico** tem direito a **um voto**.

Para ter direito a voto como um determinado tipo de ator, a pessoa/entidade deve fazer um investimento inicial de tokens a serem retidos pela DAO enquanto o direito de voto for exercido. Atores com mais poder de votação devem fazer depósitos maiores, mas em troca recebem mais influência. Depósitos menores recebem menos influência, mas são mais baratos, representando um risco menor para o investidor. Esse depósito funciona como uma garantia e pode ser confiscado pela DAO em caso de violação das regras. Caso esteja dentro das regras, o ator pode abrir mão do direito de voto e receber de volta os tokens. A imobilização dos tokens e a possibilidade de perda dos mesmos funcionam como incentivos para a conformidade com as regras da DAO, além de poder reparar danos causados pela violação das mesmas. Essas previsões devem garantir um ambiente harmônico e civilizado, adequado para as interações entre as partes interessadas.

Financiamento

Considerando que a operação e manutenção da DAO depende da compra de produtos e da contratação de serviços que só podem ser feitas utilizando moedas fiduciárias, é necessária uma entrada constante dessas moedas para que a DAO sobreviva.

A principal forma de financiamento da DAO pode ser a venda de tokens da blockchain em troca de moedas fiduciárias. As empresas, que são os maiores beneficiários do SIA LGPD, fornecem moedas fiduciárias para a DAO e em troca recebem tokens que podem ser trocados por serviços ofertados dentro do SIA, armazenados, doados ou revendidos para outros participantes da blockchain de acordo com os interesses das partes envolvidas.

A moeda fiduciária obtida pela DAO é guardada em uma instituição financeira tradicional e usada quando necessário para custear despesas como compra de servidores, equipamentos de rede e licenças de software, ou contratação de serviços como hospedagem, contadores, advogados, programadores e administradores de sistemas.

Cuidado deve ser tomado para equilibrar o valor de comercialização dos tokens e o custo necessário para fornecer os serviços pelos quais os tokens podem ser trocados. Também se faz necessária a existência de uma reserva de moeda fiduciária para oferecer liquidez para os usuários que quiserem vender tokens de volta para a DAO.

Outra possibilidade a ser explorada, a depender da legislação do local de criação da DAO, é a de investimento dos recursos excedentes, seja em ativos tradicionais ou em criptoativos. Os retornos desses investimentos podem ser transformados em melhorias na DAO ou em redução dos custos de venda dos tokens.

Outras possibilidades de financiamento são os editais governamentais e de fundações sem fins lucrativos alinhados ao propósito da DAO.

Uma possível trajetória da DAO

Etapa 1 - Criação: um grupo pequeno de desenvolvedores desenvolve o SIA, constrói a infraestrutura básica da DAO e integra as duas partes. Opcionalmente pode ser iniciado o esforço de divulgação para atrair os primeiros contribuidores.

Etapa 2 - Geração de receita: com a parte tecnológica pronta, é possível atrair os atores principais, as empresas que buscam adequação à LGPD. O custo de fornecimento dos serviços deve ser proporcional ao valor pago pelas empresas, logo a DAO se torna financeiramente viável. Com recursos financeiros é possível atrair contribuidores que precisam ser remunerados. A divulgação para contribuidores voluntários deve ser intensificada.

Etapa 3 - Atração de consumidores: com um número suficiente de empresas participando da DAO, pode ser iniciada a promoção para clientes dessas empresas, expondo os benefícios de participar do processo de adequação dessas empresas e de uma comunicação mais próxima.

Etapa 4 - Atração do Governo e da Academia: podem ser iniciados os primeiros esforços para atrair esses atores para aumentar a utilidade da DAO.

Etapa 5 - Efeitos de rede: quanto mais pessoas e entidades participam da DAO maior é sua utilidade. À medida que o número de participantes aumenta, também aumenta a promoção orgânica, tanto pelos benefícios que a DAO traz para os usuários, quanto pela necessidade de trazer mais atores semelhantes para que cada categoria seja suficientemente representada.

Etapa 6 - Ganhos de escala e capital excedente: em um determinado momento os custos de operação da DAO serão menores do que a entrada de capital, seja pelos ganhos de escala, seja pelo grande número de contribuidores voluntários. O excedente de capital pode ser diretamente investido em melhorias na própria DAO, em ativos com expectativa de

valorização ou doados para organizações alinhadas com os interesses da DAO. Caso ainda não tenha sido feito, pode ser buscado financiamento de editais públicos e ONGs para o investimento em projetos de interesse.

Análise dos atributos principais de uma DAO

Blockchain pública x Blockchain privada

Opção escolhida: Blockchain privada. Todos os participantes da DAO precisam se identificar como pessoas físicas ou jurídicas para dar legitimidade às suas ações e para que a aplicação de sanções seja possível caso ocorram violações das normas. A necessidade de aprovar a entrada de participantes na rede também reduz o risco de ingresso de agentes maliciosos. Os maiores benefícios a serem obtidos por uma DAO nesta proposta são transparência, representatividade e rapidez nos processos decisórios, tornando a blockchain privada suficiente.

Blockchain pública: qualquer entidade pode ser um usuário ou incluir um nó na rede, qualquer um pode submeter transações e participar do processo de consenso para determinar qual é o estado válido da rede. Não há necessidade de uma instituição central confiável e a blockchain garante a execução correta das transações. O registro das transações realizadas na rede são geralmente públicos, mas os usuários anônimos (ILIEVSKI, 2019).

Blockchain privada: são operadas por entidades conhecidas, onde membros ou stakeholders em um contexto de negócio operam uma rede permissionada. Existe o conceito de terceiro confiável. Uma instituição central administra os direitos de acesso de usuários e pode identificar nós, além de prover ou retirar seus direitos de transacionar (ILIEVSKI, 2019).

Topologia de rede

Opção escolhida: Descentralizada Desestruturada. Considerando os atributos buscados, é a topologia que atinge o melhor equilíbrio com Confiabilidade boa, Manutenibilidade melhor e Segurança média.

Como definido no [Technical Report FG DLT D5.1 Outlook on distributed ledger technologies](#) da ITU-T, as topologias de redes usadas em blockchains podem ser classificadas como Centralizada, Descentralizada Desestruturada, Descentralizada Estruturada e Parcialmente Descentralizada.

Os principais atributos para a DAO do SIA são: Confiabilidade (a DAO precisa manter um bom grau de disponibilidade), Manutenibilidade (possibilidade de manutenção e operação por um número pequeno de pessoas e reparo rápido) e Segurança (os participantes precisam de confiar na gestão dos ativos e no processo de votação).

Atributos menos importantes são: Escalabilidade (a rede não vai ser usada por toda a sociedade), Eficiência de Acesso a Nós (as interações não precisam ser instantâneas) e Proteção à Privacidade (todos os participantes são conhecidos).

Taxonomia

Opção escolhida: Funcional, primariamente. Os objetivos principais da DAO são criar algo novo (o SIA LGPD) e gerenciar uma atividade (desenvolvimento, a operação e a manutenção do SIA). No entanto a DAO também possui elementos associativos (causar o efeito de proteger melhor a privacidade das pessoas), transferência de valor (captar investimentos e aplicá-los na criação e melhoria do sistema) e social (organizar a própria DAO e direcionar os esforços para manter e melhorar o SIA).

De acordo com o white paper [Decentralized Autonomous Organizations: Beyond the Hype](#) do Fórum Econômico Mundial, DAOs podem ser categorizadas a partir das seguintes características:

- Objetivo:

Gerativa: buscam criar algo novo.

Associativa: buscam melhorar o funcionamento de uma comunidade ou da sociedade.

Ad hoc: buscam atingir um objetivo específico e se desfazer.

- Meios:

Atividade: buscam gerenciar uma atividade.

Transferência de valor: buscam investir capital.

Social: buscam organizar pessoas.

DLT

Opção escolhida: Hyperledger Fabric. Fornece melhor suporte para blockchains permissionadas e privadas além da possibilidade de integração com outras blockchains caso necessário.

Hyperledger: "Hyperledger Fabric é uma plataforma de registro distribuído, de grau empresarial, que oferece modularidade e versatilidade para um amplo conjunto de casos de uso da indústria.". Dentre as principais características desta DLT estão a arquitetura permissionada, alta modularidade, controle preciso de permissões de acesso a dados e um projeto para operação contínua (HYPERLEDGER FOUNDATION).

Ethereum: "é uma blockchain com um computador embutido. É a fundação para a construção de aplicativos e organizações de forma descentralizada, sem permissões e resistente a censura.

No universo do Ethereum, há um único computador canônico (chamado de Ethereum Virtual Machine, ou EVM) com um estado concordado por todos na rede Ethereum. Todos que participam da rede Ethereum (todos os nós Ethereum) mantêm uma cópia do estado deste computador. Adicionalmente, qualquer participante pode transmitir uma requisição para que este computador execute uma computação arbitrária. Sempre que esta requisição é transmitida, outros participantes na rede verificam, validam e levam adiante ("executam") a computação. Esta execução causa uma mudança de estado na EVM, que é registrada e propagada através de toda a rede.

Requisições de computação são chamadas de requisições de transação; o registro de todas as transações e o estado atual da EVM são armazenados na blockchain, que é armazenada e concordada por todos os nós.

Mecanismos criptográficos garantem que assim que transações são verificadas como válidas e adicionadas na blockchain, não podem ser alteradas depois. Os mesmos mecanismos também garantem que todas as transações são assinadas e executadas com as "permissões" (ninguém deve ser capaz de enviar ativos digitais usando a conta da Alice, exceto a própria Alice) apropriadas." (ETHEREUM FOUNDATION).

Cardano: é uma plataforma blockchain proof-of-stake. "A rede Cardano é uma infraestrutura técnica combinando nós Cardano e suas interações em um sistema unificado. A rede consiste em uma coleção de nós que se comunicam para manter o registro distribuído. Estes nós são os atores na Cardano que validam blocos, adicionam blocos à cadeia e distribuem transações.

A camada de rede é a força por trás da entrega de requerimentos de troca de informação, que inclui a difusão de novos blocos e informação de transações para estabelecer um melhor fluxo de dados. Nós Cardano mantêm conexões com pares escolhidos através de um processo customizado de seleção de pares." (CARDANO FOUNDATION).

3. Considerações finais

Ao longo da Residência Técnica foram procurados problemas relevantes para as empresas brasileiras. Este trabalho elegeu a baixa conformidade com a LGPD, enumerou motivos que justificam esta situação (como falta de dinheiro e qualificação) e propôs a criação do SIA, um sistema eletrônico para enfrentar os desafios relatados pelas empresas. Também foi feita uma proposta de criação de uma DAO que apoiasse a existência do SIA. Foram criados artefatos que permitem o início do processo de desenvolvimento de software que dá origem ao SIA e codificado um protótipo com algumas funcionalidades esperadas do produto final.

Devido às limitações de tempo e recursos disponíveis, não foi possível finalizar a implementação do SIA, mesmo que empresas tenham demonstrado interesse na utilização do produto. Também é necessário buscar o ponto de vista de empresas de diferentes segmentos (não foi possível cobrir os inúmeros existentes) e de todas as regiões do Brasil (só foram consultadas empresas do estado de Goiás). O SIA é pensado para uma aplicação generalista que cobre um caso básico. Aprimoramentos podem ser feitos para que o mesmo se adapte melhor às variações de cada organização.

Avançar a digitalização e a implementação de políticas de governança e segurança digital no Brasil são objetivos importantes neste momento que apresenta simultaneamente grande competitividade ao nível mundial e inúmeros ataques aos direitos humanos fundamentais. Os autores esperam que este trabalho contribua com as discussões a respeito das melhores práticas de tratamento de dados e que possibilite a adequação à LGPD para um número maior de empresas, fortalecendo as estruturas básicas necessárias para a existência de uma sociedade funcional.

Referências

ANPD aplica a primeira multa por descumprimento à LGPD. ANPD, 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd>. Acesso em: 21 abr. 2024.

Apenas 36% das organizações brasileiras afirmam estar totalmente aderentes à LGPD. Logicalis Group, 2023. Disponível em:

<https://www.la.logicalis.com/pt-br/noticias-apenas-36%25-das-organizacoes-brasileiras-affirmam-estar-totalmente-aderentes-a-lgpd>. Acesso em: 23 jul. 2024.

BARBEREAU, Tom et al. **Decentralised Finance's timocratic governance: The distribution and exercise of tokenised voting rights**. Technology in Society, v. 73, p. 102251, 2023.

BARBOSA, Mariana. Após polêmica, Nubank anuncia R\$ 20 milhões para medidas de combate ao racismo. O Globo, 2020. Disponível em:

<https://blogs.oglobo.globo.com/capital/post/nubank-anuncia-r-20-milhoes-em-medidas-de-combate-ao-racismo.html>. Acesso em: 21 abr. 2024.

BARRETO, Eduardo. Sikêra Jr perdeu 43 patrocinadores após fala homofóbica. Metrópoles, 2021. Disponível em:

<https://www.metropoles.com/colunas/guilherme-amado/sikera-jr-perdeu-43-patrocinadores-a-pos-fala-homofobica>. Acesso em: 21 abr. 2024.

BELARMINO, Ana Paula. O compliance na percepção de micro e pequenos empresários. **Revista Metropolitana de Governança Corporativa (ISSN 2447-8024)**, v. 5, n. 2, p. 65-65, 2020.

BRASIL. CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. Brasília, DF: Presidente da República.

BRASIL. LEI Nº 8.069, DE 13 DE JULHO DE 1990. Dispõe sobre sobre a proteção integral à criança e ao adolescente. Brasília, DF: Diário Oficial da União, 1990.

BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. Dispõe sobre o tratamento de dados pessoais. Brasília, DF: Diário Oficial da União, 2018.

CAMPOS JR, Ricardo. Quanto custa para uma micro ou média empresa se adequar às normas da LGPD?. Correio do Estado, 2020. Disponível em:

<https://correiodoestado.com.br/economia/quanto-custa-para-uma-micro-ou-media-empresa-se-adequar-as-normas-da-l/376505/#:~:text=TECNOLOGIA%20E%20SEGURAN%C3%A7A-,Quanto%20custa%20para%20uma%20micro%20ou%20m%C3%A9dia,adequar%20%C3%A0s%20normas%20da%20LGPD%3F&text=Uma%20empresa%20sul%2Dmato%2Dgrossense,que%20o%20presidente%20sancion%C3%A1%2Dla..> Acesso em: 21 abr. 2024.

Cardano network. Cardano Foundation. Disponível em:
<https://docs.cardano.org/about-cardano/explore-more/cardano-network/>. Acesso em: 16 jul. 2024.

Decentralized Autonomous Organizations: Beyond the Hype. Fórum Econômico Mundial, 2022. Disponível em:
<https://www.weforum.org/publications/decentralized-autonomous-organizations-beyond-the-hype/>. Acesso em: 16 jul. 2024.

Declaração Universal dos Direitos Humanos. ONU, 1948. Disponível em:
<https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 21 abr. 2024.

Empresas e LGPD: Cenários, desafios e caminhos. RD Station, 2021. Disponível em:
<https://d335luupugsy2.cloudfront.net/cms%2Ffiles%2F2%2F1628275980relatorio-adequacao-lgpd-rd-manar.pdf>. Acesso em: 21 abr. 2024.

Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. BBC, 2018. Disponível em:
<https://www.bbc.com/portuguese/internacional-43461751>. Acesso em: 24 jul. 2024.

Ferramenta de Diagnóstico LGPD. ABES. Disponível em:
<https://diagnosticolgpd.abes.org.br/>. Acesso em: 15 mai. 2024.

GEORGE, Kevin. The Largest Cryptocurrency Hacks So Far. Investopedia, 2024. Disponível em: <https://www.investopedia.com/news/largest-cryptocurrency-hacks-so-far-year/>. Acesso em: 16 jul. 2024.

ILIEVSKI, Andrej. **Decentralized Autonomous Organization (DAO): Utopia or Equitable Distribution?**. Iustinianus Primus Law Review, 2019.

Intro to Ethereum. Ethereum Foundation. Disponível em:
<https://ethereum.org/en/developers/docs/intro-to-ethereum/>. Acesso em: 16 jul. 2024.

IT Governance Institute. **Cobit 4.1**. ISA, 2007.

Manual Prático De Adequação À Lei Geral de Proteção de Dados para Micro e Pequenas Empresas. Instituto Brasileiro de Defesa do Consumidor, 2021. Disponível em: https://idec.org.br/system/files/ferramentas/idec_manual-lgpd_micro-pequenas-empresas.pdf. Acesso em: 15 mai. 2024.

Mapa da Digitalização das MPEs Brasileiras. ABDI, 2021. Disponível em:
https://api.abdi.com.br/file-manager/upload/files/Mapa_da_Digitaliza%C3%A7%C3%A3o_das_MPEs_Brasileiras_1_1_.pdf. Acesso em: 21 abr. 2024.

Open, Proven, Enterprise-grade DLT. Hyperledger Foundation. Disponível em: https://8112310.fs1.hubspotusercontent-na1.net/hubfs/8112310/hyperledger_fabric_whitepaper.pdf. Acesso em: 16 jul. 2024.

Outlook on distributed ledger technologies. International Telecommunication Union. Disponível em: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d51.pdf>. Acesso em: 16 jul. 2024.

Princípios para a Governança e Uso da Internet no Brasil. Comitê Gestor da Internet no Brasil, 2009. Disponível em: <https://principios.cgi.br/>. Acesso em: 21 abr. 2024.

Privacidade e proteção de dados pessoais 2021: perspectivas de indivíduos, empresas e organizações públicas no Brasil. São Paulo : Comitê Gestor da Internet no Brasil, 2022. Disponível em:

https://cetic.br/media/docs/publicacoes/2/20220817110001/privacidade_protecao_de_dados_pessoais_2021_livro_eletronico.pdf. Acesso em: 21 abr. 2024.

Segurança Da Informação Para Agentes De Tratamento De Pequeno Porte. ANPD, 2021. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf>. Acesso em: 15 mai. 2024.

Simplificando a LGPD nos Negócios. Sebrae. Disponível em: https://sebrae.com.br/Sebrae/Portal%20Sebrae/UFs/AM/Anexos/10_Cartilha%20para%20MPE_Sebrae%20AM.pdf. Acesso em: 15 mai. 2024.

Sustainable Development Goals. ONU. Disponível em: <https://sdgs.un.org/>. Acesso em: 21 abr. 2024.

The Global Risks Report 2023. Fórum Econômico Mundial, 2023. Disponível em: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf. Acesso em: 21 abr. 2024.

The Global Risks Report 2024. Fórum Econômico Mundial, 2024. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf. Acesso em: 21 abr. 2024.

UNIÃO EUROPÉIA. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data. 2016.

WRIGHT, Aaron. **The rise of decentralized autonomous organizations: Opportunities and challenges**. Stan. J. Blockchain L. & Pol'y, v. 4, p. 1, 2020.