UNIVERSIDADE FEDERAL DE GOIÁS / INSTITUTO DE INFORMÁTICA

Privacidade de Dados em Serviços Web

Requisitos Legais e Implementação de Mecanismos de Proteção

Hugo Fernandes Silva

UNIVERSIDADE FEDERAL DE GOIÁS (UFG)
INSTITUTO DE INFORMÁTICA (INF)

HUGO FERNANDES SILVA

Privacidade de Dados em Serviços Web

Requisitos Legais e Implementação de Mecanismos de Proteção

Goiânia
2025

UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE INFORMÁTICA

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO NO REPOSITÓRIO INSTITUCIONAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio do Repositório Institucional (RI/UFG), regulamentado pela Resolução CEPEC no 1240/2014, sem ressarcimento dos direitos autorais, de acordo com a Lei no 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo dos Trabalhos de Conclusão dos Cursos de Graduação disponibilizado no RI/UFG é de responsabilidade exclusiva dos autores. Ao encaminhar(em) o produto final, o(s) autor(a)(es)(as) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do Trabalho de Conclusão de Curso de Graduação (TCCG)

Nome(s) completo(s) do(a)(s) autor(a)(es)(as): HUGO FERNANDES SILVA

Título do trabalho: Privacidade de Dados em Serviços Web

Requisitos Legais e Implementação de Mecanismos de Proteção

2. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador) Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante: a) consulta ao(à)(s) autor(a)(es)(as) e ao(à) orientador(a); b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo do TCCG. O documento não será disponibilizado durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente;

- Submissão de artigo em revista científica;

- Publicação como capítulo de livro.

Obs.: Este termo deve ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **Hugo Fernandes Silva**, **Usuário Externo**, em 13/03/2026, às 14:13, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Fernando Marques Federson**, **Professor do Magistério Superior**, em 13/03/2026, às 16:44, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

HUGO FERNANDES SILVA

Privacidade de Dados em Serviços Web

Requisitos Legais e Implementação de Mecanismos de Proteção

Relatório final de Trabalho de Conclusão de Curso, apresentado à Universidade Federal de Goiás, como parte das exigências para a obtenção do título de Bacharel em Inteligência Artificial.
Orientador: Prof. Dr. Fernando Marques Federson

Goiânia
2025

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema de Bibliotecas da UFG.

SILVA, HUGO FERNANDES
Privacidade de Dados em Serviços Web [manuscrito]: Requisitos Legais e Implementação de Mecanismos de Proteção / HUGO FERNANDES SILVA. - 2025.
45 f.: 2025

Orientador: Prof. Dr. Fernando Marques Federson
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Goiás, Instituto de Informática (INF), Inteligência Artificial, Goiânia, 2025.

1. Inteligência Artificial. 2. LGPD. 3. Proteção de Dados.

I. Federson, Fernando Marques , orient. II. Título.

CDU 004

HUGO FERNANDES SILVA

Privacidade de Dados em Serviços Web

Requisitos Legais e Implementação de Mecanismos de Proteção

Relatório final de Trabalho de Conclusão de Curso, apresentado à Universidade Federal de Goiás, como parte das exigências para a obtenção do título de Bacharel em Inteligência Artificial.

Data da Aprovação: 09 de dezembro de 2025.

Prof. Dr. Fernando Marques Federson
Orientador (INF-UFG)

Prof. Dr. Aldo André Díaz Salazar
Coordenador de TCC do BIA (INF-UFG)

Prof. Dr. Anderson da Silva Soares
Coordenador do BIA (INF-UFG)

Prof. Dr. Sávio Salvarino Teles de Oliveira
(INF-UFG)

HUGO FERNANDES SILVA

Privacidade de Dados em Serviços Web

Requisitos Legais e Implementação de Mecanismos de Proteção

RESUMO

Este Relatório de Conclusão de Curso tem como objetivo reunir os resultados da minha jornada para me tornar um especialista em **Proteção de Dados**. Uma ilustração e sua narrativa descrevem os períodos de trabalho. Os Apêndices contêm os Termos de Aceite de Entrega e os resultados obtidos durante cada período de trabalho.

Palavras-chave: Inteligência artificial; LGPD; Proteção de dados.

ABSTRACT

This Course Completion Report aims to bring together the results of my journey to become an expert in **Data Protection**. An illustration and its narrative describe the work periods. The Appendices contain the Delivery Acceptance Terms and the results obtained during each work period.

Keywords: Artificial intelligence; LGPD; Data protection.

Goiânia

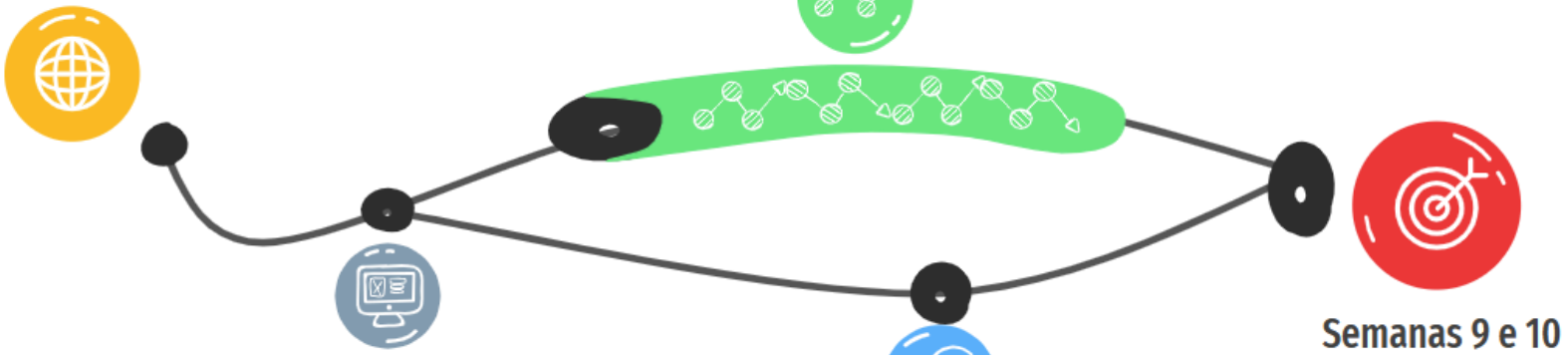
2025

Minha Jornada

Aprofundamento na legislação:
- O que se atentar ao desenvolver um app web público;
- Fluxograma "Sim Não" de *"pode ou não tratar dados?"*.

Revisão Bibliográfica: *Cloud Computing Security*

Semanas 1 , 2 e 3



Semanas 4 e 5

Diagramação (overview) de "Segurança" e definição de Roadmap

Semanas 6 e 7

Semana 8

Entrevista semi-estruturada (pesquisa qualitativa)

Semanas 9 e 10

Seleção de técnicas, mapeamento de ameaças e implementação

Hugo Fernandes Silva

Especialista (em andamento): Proteção de Dados

MINHA JORNADA

Nome: **Hugo Fernandes Silva**

Especializando: **Proteção de Dados**

Objetivo deste documento

Durante o processo da disciplina Residência em IA[1], foram gerados diversos resultados na construção da minha especialização. A cada semana, um conjunto de resultados foi formalizado por um Termo de Aceite de Entrega e avaliado por uma banca, considerando o planejado e o realizado para o período. Este documento tem como objetivo descrever esses resultados obtidos, fazendo referência aos Termos de Aceite de Entrega e seus documentos associados.

Minha Jornada

Minha Jornada de fato começou antes das **Semanas** do processo de Residência, ao ter contato com a área que me despertara interesse durante experiência com projetos na área da saúde (onde atuei como bolsista desenvolvedor) obtida com o Centro de Excelência em Inteligência Artificial (CEIA) e durante o desenvolvimento de projetos pessoais para empreender na mesma área – aproveitei a Residência para aprofundar no tópico de Proteção de Dados, momento o qual reservei para principalmente explorar nos detalhes todos os pontos a se preocupar com proteção de dados na jornada empreendedora que venho trilhando. Uma forma de descrever minha principal motivação é: o que eu entendo do medo que usuários de aplicações web possuem em relação à exposição por vazamento de dados (sejam estes causados por ataques ou acidentes).

A partir das chamadas do Computer Science, Computer Engineering, & Applied Computing (CSCE) de 2025, em especial a 24ª conferência em “Security and Management” (SAM’25), na **Semana 1** e **Semana 2** defini a área de conhecimento da minha

[1] Dez Semanas, entre setembro de 2025 e dezembro de 2025.

especialização, assim como encontrei alguns artigos basilares relacionados, através dos quais pude “afunilar” a terminologia que uso para me referir a área que me despertara interesse. A noção que obtive de palavras-chave serviu para encontrar mais artigos basilares na **Semana 3**, período que também serviu para descrever brevemente o contexto de cada trabalho encontrado, classificá-los intuitivamente usando terminologia que eu já conhecia, destacar os principais para que me trouxesse noção de uma visão geral da área, e classificar uma ordem de leitura dos trabalhos. O ranking de leitura encontra-se no **Apêndice 1.**

Um diagrama com a visão geral sobre “segurança de dados” na computação foi desenvolvido na **Semana 4** através de uma revisão bibliográfica simples (embora mais aprofundada do que nas primeiras **Semanas**). Neste diagrama, só havia espaço para informações relevantes sobre definições conceituais sobre técnicas e terminologias de diferentes autores – serviu também como uma tentativa de visualmente representar a taxonomia da área “sob as lentes” dos trabalhos lidos superficialmente desde **Semana** 1. O **Apêndice 2** mostra a abordagem que utilizei para representação de macro contextos da área e o diagrama em si.

Ainda com o diagrama explorado na **Semana** anterior, a **Semana 5** serviu para dar acabamento em sua primeira versão; ao fim desta, cheguei a conclusão (a partir da leitura que havia feito) que não era tecnologicamente viável proteger os dados de usuários do acesso de externos (principalmente se esse acesso externo é o Estado de uma nação). Portanto, recorri a proteger os dados ao menos no escopo regulamentado pelo próprio estado brasileiro, o que me levou a definir um percurso dividido em 7 etapas desde a **regulamentação nacional** até a **implementação de mecanismos de proteção de dados** em um projeto de escolha – percurso o qual tentei seguir nas **Semanas** seguintes. No **Apêndice 3** é discutido sobre a inviabilidade de completamente proteger dados de usuários, e etapas do percurso são descritas.

Ao decorrer das **Semanas 6 e 7**, aprofundei na legislação brasileira e sua interpretação, a qual me deu base para listar pontos a se atentar durante o desenvolvimento

de uma aplicação web, assim como possíveis vícios (indicadores de inviabilidade de proteger os dados seguindo “a risca” todas regulamentações). No final da **Semana 7** alcancei um fluxograma “Sim Não” (“pode ou não tratar dados?”) para classificar se pode prosseguir com o tratamento de dados do usuário num caso específico de aplicação web. O **Apêndice 4** traz observações sobre a análise da legislação e o fluxograma.

Antes que eu me “desse o luxo” de maior preocupação em mapeamento de pontos a se atentar sobre a legislação, na **Semana 8** fui atrás de pessoas que no mercado tiveram experiência com os tópicos discutidos nos parágrafos anteriores, apliquei uma entrevista semi-estruturada (pesquisa qualitativa) cujo resultado resultados me levaram a conclusão de que eu já havia mapeado mais pontos do que os necessários para se atentar na prática. O **Apêndice 5** mostra os resultados da pesquisa.

Nas últimas duas **Semanas (9 e 10),** revisitei a revisão bibliográfica das primeiras **Semanas** para destacar trabalhos que usavam mecanismos que, se implementados em conjunto e adequadamente, são relevantes para para preservar a privacidade e proteger os dados dos usuários finais de um serviço de internet em nuvem. Elenquei-os, e dei início a implementação no projeto foco da minha atual jornada empreendedora – comecei por encriptação dos dados em repouso devido a Máxima de Shannon (Princípio de Kerckhoffs): “o inimigo conhece o sistema”, logo a segurança do sigilo da informação não deve depender do quanto dificulta acesso mas sim do quanto a informação por si só é indecifrável por quem não deveria ter acesso mesmo se disposta publicamente. O **Apêndice 6** mostra os mecanismos a serem implementados e os quais até então já foram.

Em função de tudo que vivi nesta jornada, gostaria de deixar registrado que:

- como ainda estou em processo de implementar todos os mecanismos destacados nas últimas **Semanas**,
- e tendo visto durante as **Semanas 5, 6 e 7** que a prática dificilmente funciona como o planejado,

percebo que ainda estou em processo de especialização em Proteção de Dados.

A **Semana 5** foi muito importante para perceber que é inviável proteger em sua completude os dados dos usuários de uma aplicação web; e recorrendo como plano proteger dados apenas no escopo da legislação, as **Semanas 6 e 7** foram muito importantes para perceber que nem todo dispositivo da legislação, interpretado como esperado por órgãos regulamentadores, é viável de ser atendido quando se trata do desenvolvimento de uma aplicação web que trata dados de seu público.

Portanto, como o desencontro entre plano e prática vem sendo um padrão: prevejo que o restante dos mecanismos a serem implementados também pode vir a ser diferente do que fora listado na **Semana 9**. Quando finalizadas as implementações, terei concluído meu percurso definido ao longo do processo de Residência**,** me tornando um especialista.

Como mais importante, gostaria de agradecer a Deus e a minha família, estes os quais indubitavelmente foram a base para dar início a essa jornada que, se Deus quiser, abrirá espaço para muitos outros celebrarem. Agradeço também aos orientadores e à universidade por proporcionar um ambiente digno para exploração de um tópico à minha escolha. Um agradecimento especial ao Professor Doutor Sávio Salvarino Teles de Oliveira, para o qual me faltam palavras.

APÊNDICE 1

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE INFORMÁTICA

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("Gate") de aprovação: 2 de set. de 2025

Participantes da Entrega [matriculados em Residência em IA]:

Hugo Fernandes Silva

Entrega: [descrever a ENTREGA - requisitos e produtos gerados: links para textos, códigos, vídeos etc.]

Fiz uma pesquisa relacionada aos papers no tópico de Cloud Computing Security Artigos Basilares - Cloud Computing Security .

Planejamento: [descrever o que pretende fazer para realizar a próxima ENTREGA]

Realizar uma pesquisa relacionada ao quanto o Governo e a Legislação influenciam em Cloud Computing Security.

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

ACEITE DA ENTREGA:

CEDRIC LUIZ DE CARVALHO: Go!

Instituto de Informática (INF) - UFG
Alameda Palmeiras, Quadra D, Câmpus Samambaia
Fone: (62) 3521-1181 / Fax: (62) 3521-1182

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("Gate") de aprovação: 10 de set. de 2025

Participantes da Entrega [matriculados em Residência em IA]:

HUGO FERNANDES SILVA

Entrega: [descrever a ENTREGA - requisitos e produtos gerados: links para textos, códigos, vídeos etc.]

Revi artigos basilares evitando keywords desalinhadas com meu interesse.
- Queries.
- Filtro de artigos os quais presentes na maioria dos resultados.
- Leitura de sumarizações por IA.
- Conclusão.

Resultado: Artigos Basilares Revisitados de acordo com meu objetivo
Um "nome" *mais próximo* do meu interesse: "Cloud Computing end-user privacy-first mechanisms"

Planejamento: [descrever o que pretende fazer para realizar a próxima ENTREGA]

"Cherrypick" de técnicas para aplicar na prática.

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

ACEITE DA ENTREGA:

CEDRIC LUIZ DE CARVALHO: Go!

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("Gate") de aprovação: 17 de set. de 2025

Participantes da Entrega [matriculados em Residência em IA]:

HUGO FERNANDES SILVA

Entrega: [descrever a ENTREGA - requisitos e produtos gerados: links para textos, códigos, vídeos etc.]

Mais revisão, classificando os trabalhos até então: + Revisão e Classificação

Para conseguir indicar técnicas a serem implementadas
- Listei as classes em ordem decrescente de prioridade.
- Bolei uma métrica para ranquear profundidade de "skimming".
- Comecei o skimming.
  Skimming Depth Selection

Planejamento: [descrever o que pretende fazer para realizar a próxima ENTREGA]

Continuar o skimming (até ver-me apto para selecionar técnicas)

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

ACEITE DA ENTREGA:

CEDRIC LUIZ DE CARVALHO: Go!

Primeiras 3 Semanas

A revisão bibliográfica consistiu de utilizar a plataforma Consensus para um aprofundamento contextual (*deep dive*) de artigos encontrados com o ChatGPT (majoritariamente no modo Thinking para "deep researches") com o qual utilizei várias frases de busca (*queries*) – garanti se o trabalho era "clamado" ou não através de quantidade de citações através do ResearchRabbit.

As tabelas a seguir consistem do ranking de leitura para a 1ª categoria de artigos que separei intuitivamente (entre 10 categorias) após ler o nome e breve descrição atreladas a tais.

Neste início, esta categoria "Precursores" e "Definições" foi considerada a mais importante para ter noção da terminologia utilizada na área.

Desde a primeira **Semana** percebi que a área de "segurança" na computação foi majoritariamente iniciada por necessidades militares de Estados – não necessariamente continuou orbitando "militarismo" (dividiu-se em "linhas" de estudo), mas de formas diferentes do século passado continua sendo uma das principais influências até os dias de hoje.

Segurança não consiste apenas de "proteção de dados", embora seja uma palavra utilizada de forma distinta por diversos autores. Palavras relacionadas também são usadas de formas diferentes (e.g. confidencialidade, privacidade, integridade, disponibilidade, confinamento, proteção, não-identificabilidade, anonimidade, inobservabilidade).

Saltzer & Schroeder, LINDDUN, Pfitzmann & Hansen e Hoepman (vide ranking do atual **Apêndice**) são autores/trabalhos os quais utilizam terminologias com as quais mais compactuo. Anderson com "Security Engineering (2020)" (vide tabelas de ranking do atual **Apêndice**) é um que devo mencionar também, mas mais por trazer uma visão abrangente do que "segurança" (como "esfera do conhecimento") de fato é; e menos por moldar a terminologia que utilizo – são todos de distintas nacionalidades, embora todos utilizem a língua inglesa para nomenclatura, e portanto é como utilizarei também.

No mais, trago como observação que este trabalho parte do escopo do que uma pessoa jurídica deveria se atentar ao buscar preservar a privacidade dos usuários de sua aplicação web; e que tal aplicação opera sobre computação em nuvem (*cloud computing* –

como definido em Above the Clouds: A Berkeley View of Cloud Computing), e que portanto leva em consideração a proteção dos dados do usuário final da aplicação mesmo se a própria cloud estiver comprometida.

Precursors: Ranked (desc)

Rank	Work (year)	Citations	Norm year	Score
4	Saltzer & Schroeder (1975)	2,080	0.2759	**573.79**
1	RBAC (1996)	5,591	1.0000	**5591.00**
2	Clark–Wilson (1987)	1,093	0.6897	**753.79**
3	Bell–LaPadula (1976)	1,850	0.3103	**574.14**
5	Denning (1976)	1,807	0.3103	**560.79**
6	Biba (1977)	1,129	0.3448	**389.31**
7	Lampson (1973)	1,323	0.2069	**273.72**
8	Ware (1967)	83	0.0000	**0.00**

Definitions: Ranked (desc)

Rank	Work (year)	Citations	Norm year	Score
2	“Hey, You, Get Off of My Cloud” (CCS’09) (2009)	2,008	0.4211	**845.47**
4	LINDDUN privacy threat taxonomy (2011) – Lightweight approach – Tutorial	374	0.5263	**196.84**

6	Web tracking defenses & partitioning (Bujlow) (2015)	296	0.5789	**171.37**
14	Anderson, *Security Engineering* (2001)	1,490	0.0000	**0.00**
5	Sabelfeld & Myers' Information Flow Control survey (2003)	1,814	0.1053	**190.95**
1	Above the Clouds: A Berkeley View of Cloud Computing (2009)	5,331	0.4211	**2244.63**
11	IETF: encryption at rest/in transit, etc. (RFC 6973 and RFC 3552)	57	0.6316	**36.00**
	Privacy By Design, Cavoukian			
8	Engineering Privacy by Design (2011) Gurses	179	0.5263	**94.21**
7	Privacy Design Strategies (2014) Hoepman	234	0.6842	**160.11**
10	Kaaniche & Laurent PETs taxonomy (2020)	47	1.0000	**47.00**
3	Pfitzmann & Hansen terminology (2010) A terminology for talking about privacy by data minimization:Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management	527	0.4737	**249.63**
9	Heurix et al. PETs taxonomy (2015)	79	0.7368	**58.21**
12	NIST Privacy Engineering Objectives (2017)	42	0.8421	**35.37**
13	Privacy Patterns catalogs (2006)	71	0.2632	**18.68**

APÊNDICE 2

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("Gate") de aprovação: 25 de set. de 2025

Participantes da Entrega [matriculados em Residência em IA]:

Hugo Fernandes Silva

Entrega: [descrever a ENTREGA - requisitos e produtos gerados: links para textos, códigos, vídeos etc.]

Tópico foco:

- Mecanismos de privacidade embutidos em servidores de aplicações web em nuvem.

Diagrama:

- Security Overview.pdf

Planejamento: [descrever o que pretende fazer para realizar a próxima ENTREGA]

Mais leitura;
Mapear ameaças ao projeto no qual aplicarei os mecanismos

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

- **Mapear ameaças é parte de "selecionar técnicas".**
- **Diagrama ainda em progresso – julgo que a Semana é longa.**

ACEITE DA ENTREGA:

CEDRIC LUIZ DE CARVALHO: Go!

Diagrama de Visão Geral sobre “Segurança”

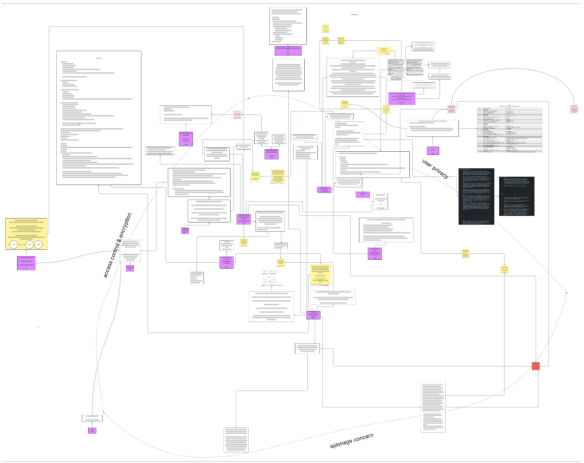
Em mérito de taxonomia, Saltzer. Em mérito de taxologia, Pfitzmann; mas em mérito de background, Anderson (vide tabelas de ranking do **Apêndice 1**).

Dividi a visão geral em 3 polos: “controle de acesso e encriptação”, “privacidade do usuário”, e “preocupação de espionagem de Estados”. Os trabalhos lidos até a **Semana 5** eram distribuíveis entre os 3:

- posicionei-os para que quanto mais fossem em direção a um polo, mais se mostraram representativos;
- também trabalhei com o eixo vertical, o qual quanto mais “baixo” → mais antigo.
- os trabalhos foram destacados de **roxo,** com blocos **brancos** de texto evidenciando informações que julguei memoráveis de cada trabalho, os **postits** foram comentários meus.

É possível perceber que todos os trabalhos se conectam de alguma forma, e o Security Engineering (2020) de Anderson fica no meio, pois é o trabalho – que dos quais pude aprofundar um pouco mais – mais conseguiu englobar as diferentes formas de atuar com segurança.

Visto que meu foco foi e é privacidade do usuário, há uma perceptível concentração de conteúdo extrapolando esse eixo. A figura 1 mostra o diagrama (ilegível, recomenda-se baixar o PDF e dar zoom para ser capaz de lê-lo: DiagramaVisãoGeralSegurança-v1.pdf).



- Figura 1 - Diagrama Visão Geral Segurança v1

APÊNDICE 3

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE INFORMÁTICA

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("Gate") de aprovação: 2 de out. de 2025

Participantes da Entrega [matriculados em Residência em IA]:

HUGO FERNANDES SILVA

Entrega: [descrever a ENTREGA - requisitos e produtos gerados: links para textos, códigos, vídeos etc.]

Tópico:

- Compliance (perante regulação brasileira) de requisitos de privacidade do usuário final de aplicações web em nuvem.

Alcancei v1 do diagrama: 4 - Security Overview - v1_021025.pdf

Defini plano de ação: 5 - Rodmap From-Regulation-To-Deploy_021025.pdf

Iniciei estudos de "requisitos guiadores".

Planejamento: [descrever o que pretende fazer para realizar a próxima ENTREGA]

Obter clareza satisfatória sobre regulação.
"Snapshot ubíquo" (neologismo: 6 - Definição de "Snapshot Ubíquo"_021025
Noção de ao menos algumas técnicas (que atendam a regulação).

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

ACEITE DA ENTREGA:

CEDRIC LUIZ DE CARVALHO: Go!

Instituto de Informática (INF) - UFG
Alameda Palmeiras, Quadra D, Câmpus Samambaia
Fone: (62) 3521-1181 / Fax: (62) 3521-1182

Inviabilidade de proteção de todos canais de acesso

A revisão bibliográfica mostrou que devido a quantidade de “side-channels”[2] possíveis de serem explorados, não é viável proteger em sua completude os dados dos usuários de uma aplicação web.

Não só isso, como também mostrou que historicamente há documentado exemplos (não tão distante; pós uso normalizado em massa de dispositivos conectados na internet) de estados de diversos países explorando side-channels para obter informações sensíveis da população, assim como implementação de “backdoors”[3] em produtos criptográficos amplamente usados no mundo todo.

Diante da realidade, resolvi proteger os dados de usuários mediante a apenas o que a legislação brasileira e suas regulamentações definem como requisito. Ilustrei um percurso com etapas desde “Regulamentação de um país” até o “Deploy” de uma aplicação web, o qual foi dividido em 6 etapas, as quais metade são para responder “O QUÊ” (o que saber antes de implementar mecanismos preservadores de privacidade num projeto) e metade para responder “COMO” (como mapear e implementá-los num projeto) – percurso o qual usei para implementar uma aplicação web de acesso público regulada sob requisitos brasileiros de proteção de dados do cidadão[4].

O QUÊ:

1. Conceitualizar regulamentações

   Listam-se regulamentações vigentes (e seus órgãos responsáveis) os quais diretamente impactam no design do sistema, identificando descrições simples as quais demonstram o que regulam e como supõe-se que podem vir a impactar no sistema em desenvolvimento.

2. Peneirar regulamentações

   Filtrar quais regulamentações são de fato relevantes, muito provavelmente é um momento para ler superficialmente, aprofundando em pontos que

[2] meios de inferir informação de um dispositivo através de canais os quais não foram desenvolvidos para disponibilizar informação.

[3] meios não documentados de contornar mecanismos de segurança; alguém que tenha conhecimento de tal consegue obter os dados “protegidos” de uma forma que os usuários comuns não conseguem.

[4] devido ao fato de ser uma abstração de “alto nível”, é um percurso que pode ser utilizado para implementar outros tipos de sistemas atendendo regulamentações de outros países.

chamam a atenção, discutindo com especialistas ou inteligência artificial. Alguém com pouca experiência em linguagem jurídica pode levar mais tempo peneirando.

No meu caso, o resultado da peneiração foi majoritariamente LGPD (Lei Geral de Proteção de Dados) e ECAD (Estatuto da Criança e do Adolescente Digital), mas com pontos a se atentar em regulamentações vizinhas (e.g. Código do Consumidor, Código Civil, a Constituição Federal em si, Marco Civil da Internet, entre outros).

3. Levantar pontos relevantes para o desenvolvedor

   Num cenário ideal, haveria dispositivos a serem destacados para o desenvolvedor sem que houvesse a necessidade dele ler outros, mas a realidade é que não existem "pontos destacáveis" – todos os dispositivos da lei afetam seriamente a interpretação contextual de dos outros; às vezes existem regulamentações posteriores que complementam a lei, as quais literalmente esclarecem como certos dispositivos devem ser interpretados. Logo, é possível perceber que este momento mais serve **para traduzir o "juridiquês" para a linguagem do desenvolvedor** do que para destacar pontos específicos. É neste momento no qual dispositivos que conflitam entre si e vícios são possíveis de ser percebidos por um especialista técnico, conclusões dúbias que só são resolvidas mediante a defesa ou num tribunal.

4. Snapshot ubíquo

   Um "mural vivo" (diagrama atualizável de tempo em tempo) onde cada bloco representa uma regulação relevante pro sistema no qual se aplicará mecanismos de privacidade. Recomendo no máximo atualizar de 6 em 6 meses, visto que há mudanças na regulamentação em média de 2 em 2 meses.

   "Snapshot" pois é apenas a representação do estado atual da regulamentação vigente (a qual pode mudar se "tirar um snapshot" outro dia) – muitas vezes tal "snapshot" não cobre todos os ângulos, mas cobre o necessário.

   "Ubíquo" pois compartilha de uma linguagem tanto jurídica quanto de domínio do desenvolvedor do sistema e do negócio.

COMO:

5. Itens de interesse

Funcionalidades e informações do sistema (ou tratadas pelo sistema) que devem ser regulamentadas (no meu caso, protegidas) de acordo com a regulamentação peneirada. Se cada bloco no snapshot ubíquo é um dispositivo "traduzido" para o domínio do negócio, nesta etapa as funcionalidades são associadas.

Importante que as funcionalidades não estejam tecnicamente descritas nesta etapa, pois os mecanismos escolhidos na próxima etapa mudam como serão tecnicamente implementadas – são apenas abstrações do que deveria funcionar considerando histórias de usuário já desenvolvidas até então.

No caso de proteção de dados, itens de interesse são melhores mapeados ao modelar ameaças do sistema – existem na academia formas diferentes de mapear tais ameaças através de diagramações, algumas mais baixo nível, outras mais alto nível.

Na revisão que fiz, LINDDUN (**L**inking, **I**dentifying, **N**on-repudiation, **D**etecting, Data **D**isclosure, **U**nawareness and **N**on-compliance) (vide tabelas de ranking do **Apêndice 1**) pareceu-me a mais completa e alinhada com terminologia a qual compactuo.

6. Mecanismos e orientações

Para atender qualquer regulamentação, há mecanismos específicos que se corretamente implementados em conjunto, atendem. No caso da proteção de dados, estamos majoritariamente falando de PETs (Privacy Enhancing Technologies). Mas elas não são o suficiente para englobar tudo a se atentar no desenvolvimento de um sistema, como Hoepman define ao discorrer sobre PDPs (Privacy Design Patterns) e PDSs (Privacy Design Strategies) (vide tabelas de ranking do **Apêndice 1**) – os quais não são mecanismos próprios, mas respectivamente abstrações conceituais destes mecanismos e orientações/regras a serem seguidas no desenvolvimento do sistema.

Essas orientações norteiam o suficiente quais mecanismos atendem. Em uma orientação podem haver vários mecanismos, os quais podem ser reutilizados em outras orientações.

Exemplo: minimização de dados é uma orientação voltada para coletar apenas os dados que o sistema realmente precisa para funcionar, um mecanismo a ser aplicado é Time To Live para informações que deveriam ser

temporárias – outros dois mecanismos que contribuem para minimização é: o PDP nunca salvar senhas decriptografáveis, e o PET local differential privacy[5]

7. Atualização de documentos

Descreve como os dados estão sendo tratados.

Após implementação dos mecanismos, deve-se atualizar documentação comprobatória que o sistema está regulado visto que a qualquer momento uma auditoria pode ser requisitada pelo jurídico (principalmente se a organização é alvo de algum processo), ou quando uma fiscalização vier a ser exercida pela autoridade reguladora.

Por lei, são informações que são necessárias estar presentes no contrato feito com o cliente (como aqueles que aceitamos em “eu concordo com a política de tratamento de dados”), portanto esses contratos também devem ser atualizados de acordo e repassados para o usuário final.

[5] dispositivos adicionam ruído aos dados enviados ao server, server só recebe dados agregados, e o ruído é o suficiente para ser difícil inferir informações sobre um indivíduo em específico em meio ao grupo, enquanto não é exagerado a ponto mudar a distribuição a ser analisada pelo server

APÊNDICE 4

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("Gate") de aprovação: 8 de out. de 2025

Participantes da Entrega [matriculados em Residência em IA]:

Hugo Fernandes Silva

Entrega: [descrever a ENTREGA - requisitos e produtos gerados: links para textos, códigos, vídeos etc.]

Tópico

- Compliance (perante regulação brasileira) de requisitos de privacidade do usuário final de aplicações web em nuvem.

Com ChatGPT, pude observar conexões entre regulações e seus guias, o que vem me dando noção do que é relevante, em progresso: (7 - Regulações Relevantes)

Me vejo na fase **"developer-relevant regulations version"** do
5 - Rodmap From-Regulation-To-Deploy_021025.pdf

Estou "travado" no ECAD 8 - ECAD - Em progresso.pdf , para o qual elenquei perguntas relevantes que me destravam (1/9 respondidas).

O alcançado até então de **"developer-relevant regulations version"** se dá pelo documento a seguir:
9 - Developer-Relevant Regulation - Em progresso.pdf

Planejamento: [descrever o que pretende fazer para realizar a próxima ENTREGA]

Obter clareza "satisfatória" sobre regulação.
"Snapshot ubíquo" (neologismo: 6 - Definição de "Snapshot Ubíquo"_021025)
Noção de ao menos algumas técnicas (que atendam a regulação).

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

Em geral,

- **o que é postit nos diagramas dessa entrega são visões pessoais,**
- **o que não é postit é a minha representação da lei *(mas não deve ser confundida com a lei em si, a qual tem poder real).***

ACEITE DA ENTREGA:

CEDRIC LUIZ DE CARVALHO: Go!

Instituto de Informática (INF) - UFG
Alameda Palmeiras, Quadra D, Câmpus Samambaia
Fone: (62) 3521-1181 / Fax: (62) 3521-1182

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE INFORMÁTICA

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("Gate") de aprovação: 16 de out. de 2025

Participantes da Entrega [matriculados em Residência em IA]:

HUGO FERNANDES SILVA

Entrega: [descrever a ENTREGA - requisitos e produtos gerados: links para textos, códigos, vídeos etc.]

Tópico

- Compliance (perante regulação brasileira) de requisitos de privacidade do usuário final de aplicações web em nuvem.

Destaquei o relevante do ECAD para minha aplicação prática 12 - ECAD_Destacado_161025.pdf

Respondi dúvidas sobre o ECAD (apoiando no que destaquei e no ChatGPT).
11 - ECAD_QuestionAndAnswer_161025.pdf

Fiz diagrama com "Quando processar dados ou não" 10 - ProcessDataYesOrNo_161025.pdf

Planejamento: [descrever o que pretende fazer para realizar a próxima ENTREGA]

"Snapshot ubíquo" (neologismo: 6 - Definição de "Snapshot Ubíquo"_021025
Noção de ao menos algumas técnicas (que atendam a regulação).

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

ACEITE DA ENTREGA:

CEDRIC LUIZ DE CARVALHO: Go!

Instituto de Informática (INF) - UFG
Alameda Palmeiras, Quadra D, Câmpus Samambaia
Fone: (62) 3521-1181 / Fax: (62) 3521-1182

Observações sobre análise da legislação

1. O que escrevi nos documentos dos termos de aceite de entrega desde a **Semana 4 até a 7** são observações que tenho sobre a legislação.
2. Essas observações às vezes vem acompanhadas de confusões que até no momento de escrita eu não havia lido o suficiente da legislação para esclarecer.
3. Tudo escrito foi uma tentativa de assimilar sob visão de projeto, visão de negócio, e visão de desenvolvedor, o que eu lia sobre a legislação.
4. Foi necessário aprendizado de termos jurídicos para assimilar de fato o conteúdo.
5. A LGPD por completo foi necessária ser assimilada, ao contrário do ECAD, o qual muito precisou ser assimilado, mas ainda assim as partes cruciais no meu caso eram apenas voltadas para os deveres de verificação de idade, aferição de idade, e recebimento de sinal de idade (visto que minha aplicação prática é de acesso público).
6. O canto superior direito do documento 11 - ECAD_QuestionAndAnswer_161025.pdf contém um caso claro de antinomia (conflito entre entre dispositivos e suas interpretações) o qual não é facilmente solucionado, e portanto reconheço como inconstitucional, ainda assim percebo que é passível de ser resolvida num ambiente jurídico com uma boa defesa.
7. O ECAD é uma lei recente e vem passando por regulamentações desde julho de 2025. Ainda há regulamentações a vir pelo Executivo, portanto os conflitos encontrados ainda podem ser corrigidos.
8.

Quanto mais aprofundei na leitura, mais percebi outras antinomias nas regulamentações, leis desatualizadas há anos, e concluí como nem todo dispositivo da legislação (interpretado como esperado por entidades reguladores) é viável de ser atendido quando se trata do desenvolvimento de uma aplicação web voltada para o público.

É notável também que irregularidades não são possíveis de serem fiscalizadas automaticamente com tecnologias atuais (e não identifiquei interesse suficiente por parte da população para o desenvolvimento destas).

A mérito de ilustração aponto que – **mesmo se a lei fosse infalível** (a qual não é) – sob a forma como os poderes estatais cumprem seus papéis, uma organização provedora de um serviço de internet o qual passa por auditoria, mesmo corretamente usando mecanismos estado da arte para preservação da proteção de dados de usuários e agindo sob boa-fé e em prol da dignidade do usuário (levando em conta o Art. 1º e 5º da Constituição Federal), é **ainda assim** passível de ser classificada como **irregular** perante **interpretação e ruído** de comunicação **entre entidades responsáveis** (e.g. entidades reguladoras, órgãos jurídicos, e defesa do investigado) **visto que a linguagem normativa** (seja a usada no tribunal ou na legislação – enquanto conjunto de signos representativos da realidade) **não abrange com precisão a complexidade dos fatos concretos envolvidos na "execução de linhas de código de uma aplicação web"** (por mais que a linguagem vigente seja o atual canal mais democrático disponível para discutir a respeito do que pode ou não ser feito na sociedade).

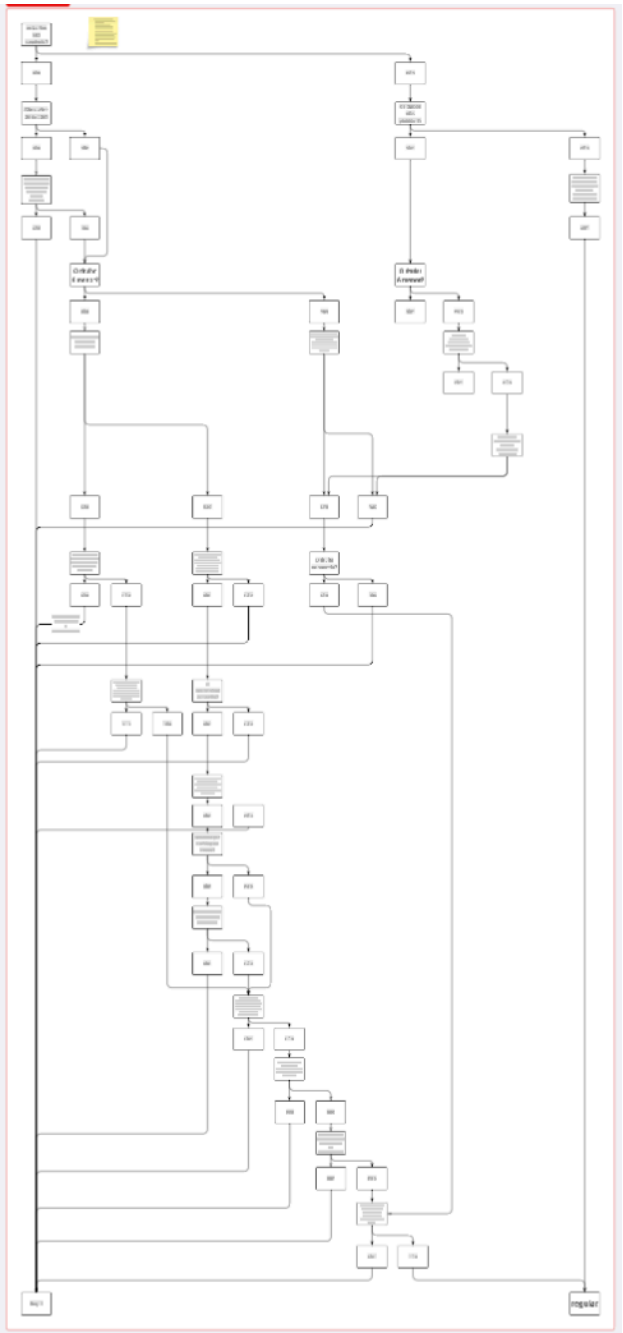
Diante da conclusão no **Apêndice 3** (i.e. não é viável proteger dados em sua completude visto a quantidade de side-channels e backdoors), e diante da conclusão no atual **Apêndice** (i.e. não é viável estar regular perante a lei visto a antinomias não solucionáveis através de critérios de conflitos), me restou não ter medo e seguir a boa-fé.

Intuitivamente percebi que prosseguir com o snapshot ubíquo (vide **Apêndice 3**) seria aprofundar mais na lei, o que levaria à mesma conclusão já encontrada, ainda assim fui atrás de um desfecho o qual foi explorado na **Semana 8** e descrito no **Apêndice 5**.

Para finalizar a **Semana 7**, recorri a um diagrama simplificado (fluxograma[6]) sobre em que caso eu poderia proceder e tratar os dados do meu usuário, e em que casos eu não poderia. Classifico-o não como Snapshot Ubíquo, mas como o suficiente como ponte entre etapa 3 e etapa 6 (considerando que para a etapa 5 assumi que todo dado de usuário

[6] Construído de forma que pouco foi considerado: aplicações com conteúdo impróprio para menores, aplicações de autoridades competentes (poder público), aplicações com viés de "rede social",e foi construído e enviesado fortemente sob a perspectiva de "aplicação web sem fins econômicos a qual permite usuários visitantes e usuários com login e é voltada para o público geral".

tratado dentro do servidor da minha aplicação seria um item de interesse a ser preservada privacidade). A figura 2 mostra o fluxograma (ilegível, recomenda-se baixar o PDF e dar zoom para ser capaz de lê-lo: 10 - ProcessDataYesOrNo_161025.pdf).



- Figura 2 - “Proceder ao processar dados? Sim ou Não?”

APÊNDICE 5

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("Gate") de aprovação: 23 de out. de 2025

Participantes da Entrega [matriculados em Residência em IA]:

Hugo Fernandes Silva

Entrega: [descrever a ENTREGA - requisitos e produtos gerados: links para textos, códigos, vídeos etc.]

Tópico

- Compliance (perante regulação brasileira) de requisitos de privacidade do usuário final de aplicações web em nuvem.

Fiz pesquisa de campo com empreendedores, especialistas em cibersegurança e investidores:
13 - Pesquisa de campo e Insights

Obtive 2 gráficos:
14 - Pergunta 1 - Preocupação com compliance desde o início da startup impede progresso.png **?**
R: Maioria: "Sim, mas faça o que podes para o compliance."

15 - Pergunta 2 - Investidores deixam de investir sem compliance.png **?**
R: Resultados balanceados, mas o "core" foi: Depende do setor e do estágio (tendendo para "não" se "seed").

Planejamento: [descrever o que pretende fazer para realizar a próxima ENTREGA]

Seleção de técnicas a utilizar para aplicar proteção de dados.

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

ACEITE DA ENTREGA:

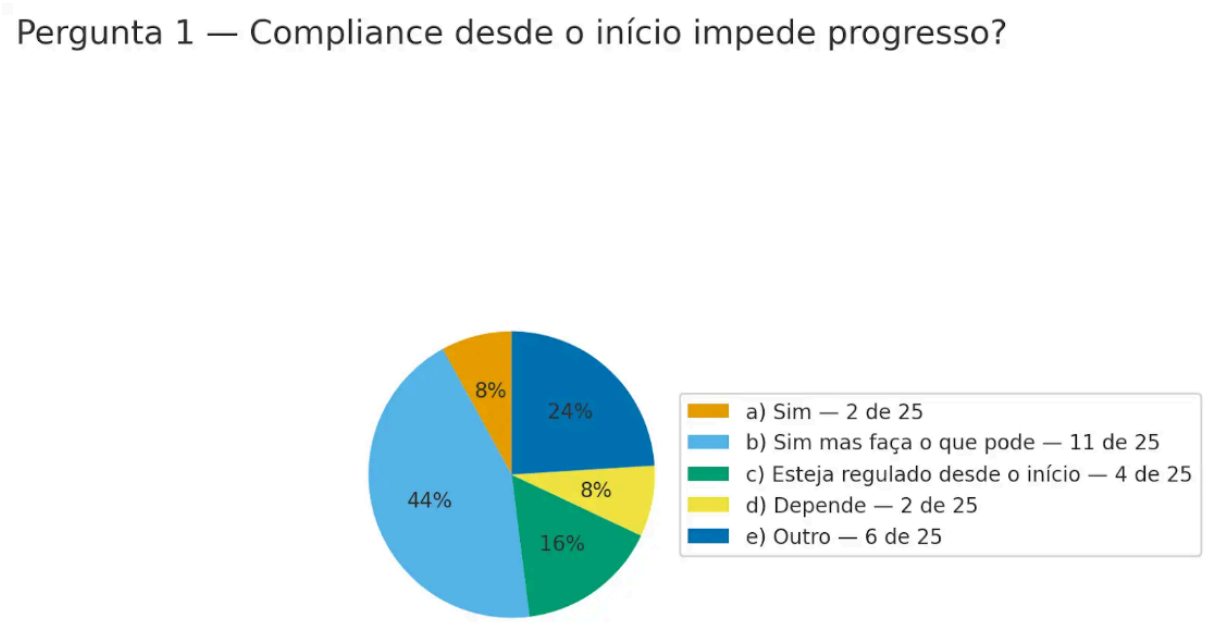
CEDRIC LUIZ DE CARVALHO: Go!

Desfecho em o que se atentar sobre a legislação

Embora minha conclusão já estivesse quase formada, busquei comparar com o único lugar onde não havia comparado ainda: pessoas com experiência na área.

Defini duas perguntas, abordei uma pesquisa qualitativa (semi-estruturada) na qual ouvi suas respostas:

1. Uma startup nascendo num setor altamente regulado, a preocupação dessa startup com compliance[7] desde o início impede o progresso dela? (Figura 3)

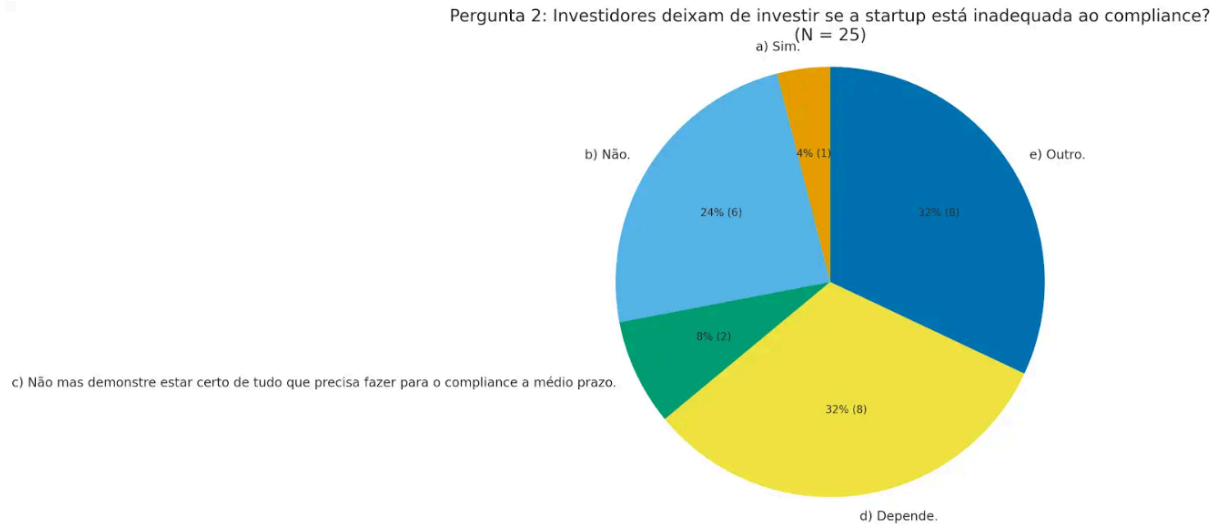


- Figura 3 - “Preocupar-se com estar regulado desde o início de um negócio impede seu progresso?”

[7] “startup com compliance” lê-se “negócio (em fase inicial) regulado perante a lei”.

A maioria das respostas foram classificadas em “Sim mas faça o que pode”, que por sinal é uma opinião que reflete a minha conclusão das **Semanas** anteriores, seguir com boa-fé e estando regular com a lei no que é possível estar regulado. Algo que no momento em que escrevo este **Apêndice** também acredito: diante da impossibilidade de seguir a legislação “à risca”, que um negócio deve fazer o possível para manter uma boa reputação.

2. Investidores deixam de "colocar dinheiro na mesa" se a startup está inadequada ao compliance? (Figura 4)



- Figura 4 - “Investidores deixam de investir no início de um negócio ainda não regulado?”

A maioria das respostas foram classificadas em “Depende” e “Outro”, representativos de que depende da área, do estágio do negócio, e de outras variáveis, assim como representativos de que um investidor deixa de investir num negócio nessas circunstâncias por causa de outros motivos que estão correlacionados com “não estar regulado” mas que não necessariamente é o fato de “não estar regulado”. Para quem está construindo o próprio negócio, há alguns insights relevantes que inferi (com minhas próprias conclusões) os quais são evidenciados no Pesquisa de campo e Insights.

APÊNDICE 6

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("Gate") de aprovação: 5 de nov. de 2025

Participantes da Entrega [matriculados em Residência em IA]:

Hugo Fernandes Silva

Entrega: [descrever a ENTREGA - requisitos e produtos gerados: links para textos, códigos, vídeos etc.]

Tópico

- Compliance (perante regulação brasileira) de requisitos de privacidade do usuário final de aplicações web em nuvem.

Revisitei minha revisão e destaquei artigos relevantes para seleção das técnicas:
1 - + Revisão e Classificação_250925

"Discuti" com ChatGPT para filtrar algumas técnicas
Brainstorm-Mechanisms-Filtering.pdf

Selecionei técnicas com base na minha stack (dividi-as em "prioridade" e "outros"):
Mecanismos para Aprimorar Privacidade dos Dados na Minha Stack

Planejamento: [descrever o que pretende fazer para realizar a próxima ENTREGA]

Por em prática!

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

Algumas técnicas podem ser adicionadas e outras removidas ao longo da prática.

ACEITE DA ENTREGA:

CEDRIC LUIZ DE CARVALHO: Go!

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE GOIÁS
INSTITUTO DE INFORMÁTICA

Termo de Aceite de Entrega

Objetivo deste documento

Este documento faz parte do Processo da disciplina Residência em IA e tem como objetivo formalizar o aceite da entrega considerando o planejado e o realizado para o período.

Data da Reunião ("Gate") de aprovação: 13 de nov. de 2025

Participantes da Entrega [matriculados em Residência em IA]:

HUGO FERNANDES SILVA

Entrega: [descrever a ENTREGA - requisitos e produtos gerados: links para textos, códigos, vídeos etc.]

No tópico:

- Data protection compliance mechanisms

1) Considerei ameaças da aplicação prática e mudei prioridades de implementação:
   Mecanismos para Aprimorar Privacidade dos Dados na Minha Stack

2) Implementei Encryption at Rest.

Planejamento: [descrever o que pretende fazer para realizar a próxima ENTREGA]

- **Infográfico**
- **Mais implementações**

Observação: [caso precise fazer alguma observação, de qualquer "natureza"]

ACEITE DA ENTREGA:

CEDRIC LUIZ DE CARVALHO: Go!

Instituto de Informática (INF) - UFG
Alameda Palmeiras, Quadra D, Câmpus Samambaia
Fone: (62) 3521-1181 / Fax: (62) 3521-1182

Mecanismos e orientações

Visto as conclusões dos **Apêndices 3, 4 e 5**, fui da etapa 3 do percurso para etapa 6 (vide **Apêndice 3**) com a visão “farei o viável para proteger os dados dos meus usuários perante ameaças realistas”.

Elenquei os seguintes mecanismos/orientações, os quais resolvem bastante da privacidade de dados de usuário caso bem implementados na aplicação a qual já tenho parcialmente desenvolvida:

1. Encriptação de dados em repouso (orientação)
2. Autenticação segura (orientação)
3. Autorização segura (orientação)
4. Visita segura (orientação – atrelada ao domínio do negócio)
5. Encriptação de dados em trânsito (orientação)
6. Isolamento de rede (orientação)
7. Minimização de dados (orientação)
8. Bloqueamento de cross origin (mecanismo)
9. Autodestruição (mecanismo)
10. Deploy com autenticação segura (orientação)
11. Mitigação de vulnerabilidades de side-channels (orientação)
12. Configuração de cookies para evitar cliente comprometido (mecanismo).

Defini outros mecanismos/orientações, as quais também tenho interesse em desenvolver, mas são custosos e/ou consomem tempo inviável e/ou exigem reestruturação da minha aplicação por inteiro (em troca de aprimorar apenas pequena parte da privacidade do usuário).

13. Mitigação de vulnerabilidade de outros side-channels (orientação)
14. Dados falsos (orientação – atrelada ao domínio do negócio)
15. Encriptação ponta a ponta (mecanismo)
16. Attribute based encryption (mecanismo)
17. Execução segura em Nuvem (orientação)
18. Aprendizado federado (mecanismo)

19. Local Location Differential Privacy (mecanismo – atrelada ao domínio do negócio)
20. MimbleWimble (mecanismo – atrelada ao domínio do negócio)
21. Oblivious HTTP (mecanismo)
22. Detecção de anomalia (mecanismo – atrelada ao domínio do negócio)
23. Logging censurando Informações Pessoais Identificáveis (mecanismo)

As orientações listadas contém várias técnicas distintas; as hipóteses que tracei até então foram contraditas, e tendo em vista o padrão, suponho que essas técnicas também não serão todas implementadas, e talvez surjam mais no percurso.

Até então, a orientação implementada foi “1. encriptação de dados em repouso”, seguindo o princípio de Kerckhoffs (vide Minha Jornada) ao utilizar os seguintes mecanismos:

- XChaCha20-Poly1305 para encriptação;
- HKDF-SHA-256 para derivação de uma chave para cada tipo de uso;
- Blind Index (HMAC-SHA-256) para campos consultáveis;
- Encriptação Estruturada para consultar informações sem decriptá-las.