# 

Projeto de Graduação em Computação I

PROJETO DE EXECUÇÃO – IDENTIFICAÇÃO CIVIL DIGITAL

Orientador: Prof. Dr. Carlos Alberto Kamienski

Aluno: Kauan Manzato do Nascimento

Santo André – SP

Julho de 2021

**1 - Introdução**

O Projeto de Graduação em Computação (PGC) é um trabalho teórico ou aplicado que tem dois objetivos básicos: a) complementar e estender a formação do aluno, permitindo o seu aperfeiçoamento e aprofundamento em um determinado tema pertencente a uma das linhas de pesquisas existentes no CMCC, preparando-o assim para um Programa de Pós-Graduação ou ainda para a inovação em um ambiente corporativo e b) avaliar o desempenho do discente tendo em vista os objetivos gerais do curso.

Este trabalho em específico trata sobre o problema da identificação civil no Brasil, suas consequências e propõe como solução um sistema digital que faz a identificação e a autenticação dos cidadãos brasileiros baseado na infraestrutura de chave pública (PKI) e no sistema atual de identificação digital da Estônia, sendo avaliado pelos seguintes critérios:

* **Eficácia:** se o sistema cumpre os objetivos designados;
* **Eficiência:** quantidade de recursos utilizados para implementar o sistema e mantê-lo;
* **Autenticidade:** a solução deve garantir que as pessoas identificadas são realmente quem elas afirmam ser;
* **Inclusão social:** a solução deve ser simples o suficiente para ser implementada em regiões com baixos índices de desenvolvimento humano e atingir o máximo de pessoas possível;
* **Interoperabilidade:** a solução precisa definir um padrão com abrangência nacional e que permita a interação entre os diferentes órgãos públicos.

**2 –** **Justificativa**

Com o advento da pandemia do novo coronavírus (Covid-19) em 2020, o Governo Federal brasileiro concedeu um benefício chamado Auxílio Emergencial cujo objetivo é minimizar o impacto da crise do vírus na população de baixa renda, de trabalhadores informais, de microempreendedores individuais e contribuintes individuais do INSS (Instituto Nacional do Seguro Social) (Brasil, 2020). Entretanto, para receber o benefício, a pessoa precisa cumprir uma série de requisitos, como previsto na Lei nº 13.982/2020.

O cadastro dos dados e a liberação dos valores do auxílio à população se dá por meio de um software para smartphones, chamado Caixa Tem: a pessoa baixa o aplicativo no dispositivo, informa seus dados pessoais (autodeclaração) e aguarda a aprovação do Ministério da Cidadania (CAIXA, 2021).

Desde o início do cadastramento, as pessoas têm relatado situações em que sujeitos receberam o benefício sem cumprir os requisitos, e situações em que alguém usou os dados de outra pessoa para receber o benefício. Estas situações caracterizam o delito de estelionato, previsto no artigo 171 do Código Penal (BRASIL, 1940) (ARAÚJO; ANDRETTA, 2020).

Este é mais um exemplo dos inúmeros casos de fraude envolvendo o Cadastro de Pessoas Físicas (CPF), registro instituído em 1965 por meio da Lei 4.862, de 29 de novembro de 1965, projetado exclusivamente para a verificação da contribuição do Imposto de Renda de Pessoa Física (IRPF). Atualmente, o CPF é mantido pela Receita Federal do Brasil e, na prática, utilizado para identificação civil, como uma alternativa ao Registro Geral (RG).

Em outras palavras, o CPF é antigo (mais de 50 anos desde a sua instituição), carecendo da eficiência que a tecnologia atual pode oferecer, e é usado para fins não coerentes com o projeto original, como a identificação dos cidadãos e suas relações com órgãos públicos, a exemplo do projeto de lei 1422, de 2019. E isso se dá porque o Brasil carece de um sistema nacional para a identificação civil.

O Registro Geral (RG), ou carteira de identidade, é um documento utilizado para a identificação de pessoas físicas nascidas no Brasil e tem validade nacional (BRASIL, 1983). Entretanto, existem alguns problemas associados a este documento:

* Cada unidade federativa é responsável por emitir uma carteira de identidade diferente, sem nenhuma ligação entre si. E, como são 27 unidades federativas, cada cidadão brasileiro pode ter 27 RGs diferentes.
* Os dados que constam no documento variam de acordo com o órgão responsável pela emissão, ou seja, existe uma falta de padrão no documento ao longo do tempo.

Além do CPF e do RG, ainda existem outros documentos que podem ser usados para identificar uma pessoa física, como a Certidão de Nascimento, o Título de Eleitor, a Carteira de Habilitação (CNH) e o Registro Nacional de Estrangeiro (RNE) (usado por estrangeiros). Podemos então enumerar os problemas do sistema de identificação civil atual:

* Falta de padrão
* Falta de centralização
* Problemas de projeto
* Soluções improvisadas e temporárias (uso do CPF para identificação)
* Sistema complexo e burocrático

Esses problemas geram consequências sérias como fraudes, inconsistência de dados e vazamentos de dados pessoais (ROHR, 2021).

**3 - Objetivos**

3.1 – OBJETIVO GERAL

O objetivo do PGC é projetar, desenvolver e implementar um sistema de informações que permita a identificação e a autenticação das pessoas de forma a evitar fraudes, vazamentos de dados e inconsistência dos dados.

3.2 – OBJETIVOS ESPECÍFICOS

São objetivos específicos:

1. Criar uma infraestrutura de chave pública (PKI) simples;
2. Configurar os seguintes dados usados na autenticação, simulando a emissão de um ID card
   1. PIN, Chave Privada (ECC) e Certificado Digital (X.509) relativos à autenticação
   2. PIN, Chave Privada (ECC) e Certificado Digital (X.509) relativos à assinatura digital
   3. Dados sigilosos: Nome completo, CPF, Sexo, Foto, Impressão Digital, Filiação, Naturalidade
   4. Local de emissão
   5. Data de emissão
   6. Data de validade
3. Implementar um banco de dados que inclua informações sobre as pessoas registradas e seus respectivos ID cards (carteiras de identidade) emitidos
   1. Os dados sigilos só podem ser acessados por autoridades com permissão ou a própria pessoa
4. Implementar o mecanismo de autenticação

**4 – Proposta**

A proposta do PGC é desenvolver um sistema de identificação e autenticação por meio de uma infraestrutura de chave pública (PKI) e smart cards, com base no sistema estoniano de identificação e autenticação.

A ideia é substituir as carteiras de identidade e os sistemas de identificação atuais que usam apenas o CPF como informação principal por um sistema de autenticação e identificação de dois fatores: um dos fatores é a possessão do smart card, dispositivo simples que guarda chaves privadas e certificados digitais, usados para a identificação e a autenticação; e o uso de senhas, conhecidas apenas pela pessoa que se quer identificar.

**5 – Metodologia**

O Projeto de Graduação em Computação (PGC) representa o momento em que o estudante demonstra as competências e habilidades desenvolvidas no curso em um projeto de maior complexidade, no qual ele possa aplicar de modo integrado todos os conteúdos e técnicas com as quais teve contato. O aluno deve mostrar capacidade de avaliar a tecnologia existente de maneira crítica, bem como de buscar novas tecnologias de forma independente.

O PGC é um trabalho individual ou em grupo, dividido em três partes (PGC I, PGC II e PGC III), cada parte com carga didática de oito créditos.

O discente possui as seguintes obrigações gerais:

* Informar-se sobre as normas e regulamentos do PGC
* Cumprir as normas e regulamentos do PGC
* Verificar as atividades e prazos de orientação e cumpri-los
* Providenciar todos os documentos solicitados pelo Coordenador de PGC, dentro dos prazos por ele estabelecidos.

No PGC I, o discente tem as obrigações:

* Entregar a Declaração de Orientação do orientador, junto com os formulários contendo o título do projeto, um resumo da proposta de trabalho e o nome do componente com a respectiva assinatura;
* Entregar, na forma e prazo definido pelo Coordenador do PGC, o Projeto de Execução do PGC
* Cumprir as atividades estabelecidas no Projeto de Execução, estabelecidas em conjunto com o orientador

No PGC II, o discente tem as obrigações:

* Cumprir as atividades estabelecidas no Projeto de Execução, estabelecidas em conjunto com o orientador
* Entregar, na forma e no prazo estabelecidos pelo Coordenador do PGC os seguintes documentos:
  1. Formulário de avaliação parcial
  2. Formulário de avaliação final
  3. Versão preliminar do PGC

E, no PGC III, o discente tem as obrigações:

* Cumprir as atividades estabelecidas no Projeto de Execução e/ou Versão Preliminar do PGC, estabelecidas em conjunto com o orientador
* Entregar, na forma e no prazo estabelecidos pelo Coordenador do PGC os seguintes documentos:
  1. Declaração de Orientação
  2. Formulário de avaliação parcial
  3. Versão final do PGC, que será encaminhada à banca examinadora

# 6 – Cronograma

O tempo total deste trabalho é estimado em 12 meses (três quadrimestres). Ao final deste período, o resultado é a implementação da proposta descrita acima e o documento que será entregue à banca examinadora. Baseando-se na definição de PGC (projeto pedagógico) e nos objetivos da proposta, podem ser desenvolvidas diferentes atividades que poderão ser acompanhadas no cronograma do projeto.

1. Estudo de Conceitos Básicos
   1. Entender o problema: como funciona a identificação de pessoas no Brasil, as vulnerabilidades do processo atualmente, propostas feitas pelo governo para resolver, causas e consequências do problema, e contexto.
   2. Estudar soluções existentes: procurar na literatura problemas similares e soluções propostas, entender as soluções e compará-las entre si, verificar a viabilidade.
   3. Estudar os conceitos básicos de governança pública: (identificação, responsabilidade com os dados e as pessoas); e como esses aspectos estão presentes no Brasil.
   4. Estudar conceitos fundamentais de segurança da informação e criptografia: autenticação, confidencialidade e integridade (CIA), criptografia de chave pública, infraestrutura de chave pública, assinatura digital, certificado digital, fatores de autenticação.
2. Desenvolvimento do projeto de execução
   1. Desenvolver a parte “Introdução”: descrição breve do trabalho como um todo, do problema e da solução;
   2. Desenvolver a parte “Justificativa”: contextualização, descrição de causas e consequências, e relevância do problema;
   3. Desenvolver a parte “Objetivos”: enumeração dos objetivos gerais e específicos;
   4. Desenvolver a parte “Proposta”: descrição da proposta;
   5. Desenvolver a parte “Metodologia”: explicação do método utilizado para avaliar o aluno, o projeto e o documento;
   6. Desenvolver a parte “Cronograma”: descreve quando e por quanto tempo cada atividade será desenvolvida;
   7. Desenvolver a parte “Referências Bibliográficas”: referências bibliográficas dos conteúdos utilizados para desenvolver o documento.
3. Implementação da proposta
   1. Implementar uma infraestrutura de chave pública (PKI);
   2. Simular a emissão de um cartão de identidade;
   3. Implementar um banco de dados para armazenar dados pessoais;
   4. Implementar um mecanismo de autenticação;
   5. Realizar testes com a proposta e anotar os resultados, de acordo com os critérios de avaliação descritos.
4. Desenvolvimento do documento final e entrega do sistema
   1. Desenvolver a parte “Introdução”;
   2. Desenvolver a parte “Justificativa”;
   3. Desenvolver a parte “Objetivos”;
   4. Desenvolver a parte “Proposta”;
   5. Desenvolver a parte “Revisão Bibliográfica”: são descritos as ferramentas, as plataformas, os serviços e as tecnologias utilizados para desenvolver e implementar a proposta;
   6. Desenvolver a parte “Resultados”: nesta parte, os testes com a proposta são feitos e os resultados são mostrados e analisados;
   7. Desenvolver a parte “Conclusão e trabalhos futuros”;
   8. Desenvolver a parte “Referências bibliográficas”;

7.1 – CRONOGRAMA DE ATIVIDADES

O cronograma de atividades previsto para este projeto é apresentado na Tabela 1. As linhas correspondem às atividades e suas respectivas ações, enquanto as colunas correspondem aos meses do projeto, com o mês 1 sendo mês inicial do projeto. As atividades podem se sobrepor, já que várias atividades podem ser desenvolvidas em paralelo.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ATIVIDADE** | | **MÊS** | | | | | | | | | | | |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** |
| Atividade 1 | 1.1 |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.2 |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.3 |  |  |  |  |  |  |  |  |  |  |  |  |
| 1.4 |  |  |  |  |  |  |  |  |  |  |  |  |
| Atividade 2 | 2.1 |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.2 |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.3 |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.4 |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.5 |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.6 |  |  |  |  |  |  |  |  |  |  |  |  |
| 2.7 |  |  |  |  |  |  |  |  |  |  |  |  |
| Atividade 3 | 3.1 |  |  |  |  |  |  |  |  |  |  |  |  |
| 3.2 |  |  |  |  |  |  |  |  |  |  |  |  |
| 3.3 |  |  |  |  |  |  |  |  |  |  |  |  |
| 3.4 |  |  |  |  |  |  |  |  |  |  |  |  |
| 3.5 |  |  |  |  |  |  |  |  |  |  |  |  |
| Atividade 4 | 4.1 |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.2 |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.3 |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.4 |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.5 |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.6 |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.7 |  |  |  |  |  |  |  |  |  |  |  |  |
| 4.8 |  |  |  |  |  |  |  |  |  |  |  |  |

Tabela 1 – Cronograma de atividades

**7 – Referências Bibliográficas**

ARAÚJO, Carla; ANDRETTA, Filipe. **Mentir para receber os R$ 600 é fraude e pode dar mais de 6 anos de prisão.** UOL Economia, [S. l.], 4 jun. 2020. Disponível em: <https://economia.uol.com.br/noticias/redacao/2020/06/04/auxilio-emergencial-crime-fraude-estelionato-r-600.htm>. Acesso em: 15 jul. 2021.

BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940**. Rio de Janeiro. Disponível em <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 14 jul. 2021.

BRASIL. **Lei nº 4.862, de 29 de novembro de 1965**. Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L4862.htm>. Acesso em: 15 jul. 2021.

BRASIL. **Lei nº 7.116, de 29 de agosto de 1983.** Assegura validade nacional às Carteiras de Identidade, regula sua expedição e dá outras providências. Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/1980-1988/l7116.htm>. Acesso em: 29 jul. 2021.

BRASIL. **Lei nº 9.454, de 7 de abril de 1997**. Institui o número único de Registro de Identidade Civil e dá outras providências. Brasília. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9454.htm>. Acesso em: 14 jul. 2021.

BRASIL. **Decreto n.º 7.166, de 5 de maio de 2010**. Cria o Sistema Nacional de Registro de Identificação Civil, institui seu Comitê Gestor, regulamenta disposições da Lei no 9.454, de 7 de abril de 1997, e dá outras providências. Brasília. Disponível em: <http://planalto.gov.br/ccivil_03/_ato2007-2010/2010/Decreto/D7166.htm>. Acesso em: 15 jul. 2021.

BRASIL. **Lei nº 13.982, de 2 de abril de 2020**. Brasília. Disponível em: [http://www.planalto.gov.br/ccivil\_03/\_ato2019-2022/2020/lei/l13982.htm#](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l13982.htm). Acesso em: 14 jul. 2021.

BRASIL. Congresso Nacional. **Projeto de lei 1422, de 2019**. Institui o Cadastro de Pessoas Físicas (CPF) como número suficiente para identificação do cidadão nos bancos de dados de serviços públicos, altera dispositivos da Lei nº 13.460, de 26 de junho de 2017, e dá outras providências. Brasília. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node0hc634df4zwgpb2a5uedtixl4675198.node0?codteor=1718365&filename=PL+1422/2019>. Acesso em: 15 jul. 2021.

CAIXA ECONÔMICA FEDERAL. **Auxílio Emergencial 2021**. CAIXA. Disponível em: <https://www.caixa.gov.br/auxilio/auxilio2021/Paginas/default.aspx>. Acesso em: 14 jul. 2021.

Receita Federal. **Perguntas e Respostas**. Disponível em: <https://receita.economia.gov.br/orientacao/tributaria/cadastros/cadastro-de-pessoas-fisicas-cpf/assuntos-relacionados/perguntas-e-respostas>. Acesso em: 29 jul. 2021.

ROHR, Altieres. **Megavazamentos de dados expõem informações de 223 milhões de números de CPF**: **Dezenas de arquivos foram disponibilizados publicamente e colocados à venda por criminosos.**. G1 - Economia. 25/01/2021. Disponível em: <https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/01/25/vazamentos-de-dados-expoem-informacoes-de-223-milhoes-de-numeros-de-cpf.ghtml>. Acesso em: 29 jul. 2021.

VINHAS, Ana. **Em um ano, PF abre 931 inquéritos sobre fraude do auxílio: Desde o início do programa, em abril de 2020, foram realizadas 332 operações, 44 prisões e R$1 milhão de bens apreendidos.** R7, [S. l.], 15 de maio de 2021. Disponível em: <https://noticias.r7.com/economia/em-um-ano-pf-abre-931-inqueritos-sobre-fraude-do-auxilio-15052021>. Acesso em: 14 jul. 2021.