



Centro Universitário de Brasília (CEUB)

Faculdade de Tecnologia e Ciências Sociais Aplicadas (FATECS)

Beatriz de Abreu Soares Schmitz - 22353779

João Luiz Veríssimo Falcão Rodrigues - 22353899

Júlia Sanches Dourado - 22353838

Yuri D' Alessandro Cunha de Carvalho - 22351384

**Projeto Integrador I - Relatório de conformidade com princípios de segurança e
privacidade**

Brasília

2025

Beatriz de Abreu Soares Schmitz

João Luiz Verissimo Falcão Rodrigues

Júlia Sanches Dourado

Yuri D' Alessandro Cunha de Carvalho

Relatório de conformidade com princípios de segurança e privacidade

Atividade desenvolvida à Faculdade de Tecnologia e Ciências Sociais Aplicadas (FATECS), do Centro Universitário de Brasília (CEUB) como parte integrante do currículo da disciplina Gerência de Projetos de TI, da graduação em Ciência da computação
Professora responsável: Kadidja Valéria Reginaldo de Oliveira.

Brasília

2025

SUMÁRIO

1 - INTRODUÇÃO	04
2 -PRÁTICAS DE SEGURANÇA E PRIVACIDADE	05
2.1 Minimização de Dados	
2.2 Privacidade	
2.3 Segurança da Informação	
2.4 Armazenamento Seguro	
2.5 Transparência e Consentimento	
2.6 Prevenção à Discriminação	
3 -REFERÊNCIAS	07

INTRODUÇÃO

O projeto Conexão Solidária adota princípios de segurança e privacidade rigorosamente alinhados à Lei Geral de Proteção de Dados Pessoais (LGPD), Lei (13.709/2018), com o objetivo de priorizar a proteção de informações relacionadas à inclusão de pessoas neurodivergentes no mercado de trabalho. O sistema opera primariamente com dados institucionais de ONGs e empresas, evitando a coleta de dados pessoais sensíveis dos usuários autistas, o que reforça o compromisso com a conformidade legal, a ética e a responsabilidade.

PRÁTICAS DE SEGURANÇA E PRIVACIDADE

As seguintes práticas são implementadas para assegurar a conformidade com a legislação e manter um ambiente seguro para todas as partes envolvidas:

2.1 Minimização de Dados

- É coletado o necessário para o mapeamento de empresas com vagas inclusivas e disponíveis, seguindo o princípio da necessidade previsto na LGPD.

2.2 Privacidade

- A interação inicial é anônima, não sendo solicitada qualquer informação pessoal dos usuários neurodivergentes.

2.3 Segurança da Informação

2.3.1 Autenticação via API: Utilização de Interfaces de Programação de Aplicações para garantir a autenticidade das comunicações.

2.3.2 Criptografia de credenciais: Medida de segurança para proteger o acesso a contas e sistemas.

2.3.3 Prevenção contra SQL Injection: Implementação de técnicas de codificação e validação para mitigar vulnerabilidades de injeção de código.

2.3.4 Controle de acesso ao banco de dados: Restrições e permissões gerenciadas para garantir que apenas pessoal autorizado acesse as informações armazenadas.

2.4 Armazenamento Seguro

2.4.1 Autenticação de 2 fatores: Reforço na segurança para acesso a repositórios e sistemas.

2.4.2 Backups: Realização de cópias de segurança para garantir a recuperação de dados em caso de falhas.

2.4.3 Repositórios privados: Utilização de ambientes restritos para armazenamento de arquivos considerados sensíveis.

2.5 Transparência e Consentimento

2.5.1 Qualquer eventual coleta futura de dados pessoais será realizada mediante o consentimento explícito dos responsáveis, conforme exigido pela LGPD.

2.5.2 É garantida a possibilidade de exclusão total dos dados pelo usuário a qualquer momento.

2.6 Prevenção à Discriminação

2.6.1 O sistema não realiza o registro de perfis individuais de pessoas neurodivergentes.

2.6.2 Não há exposição de dados que possam identificar ou comprometer a privacidade dos usuários.

REFERÊNCIAS

BRASIL. Lei (13.709/2018). Dispõe sobre a proteção de dados pessoais e altera a Lei (12.965/2014). Diário Oficial da União: seção 1, Brasília, DF, p. 59, 14 ago. 2018.