faEtapa 1

Conhecimento da Legislação de Segurança da Informação

1 Equipe de trabalho

- **Davi Mateus Gaio** – 1581196
- **Gabrielle Almeida** – 879347
- **Guilherme Augusto Andrade da Silva Borges** – 894766
- **Luiz Otávio da Silva Pereira** – 883502
- **Nicolas Miller** – 806349
- **Roberto Semantob Junior** – 890262

2 Compreendendo a organização

A GitLab, atuando no setor de tecnologia, destaca-se por oferecer uma plataforma unificada que cobre todo o ciclo de vida do DevOps, integrando desde o planejamento e desenvolvimento de software até a implantação, monitoramento e gestão de segurança de aplicações. Seu principal objetivo é simplificar e otimizar processos para equipes de desenvolvimento, operações e segurança, eliminando a fragmentação de ferramentas e promovendo colaboração eficiente entre áreas tradicionalmente isoladas.

Com foco em automação e integração contínua, a plataforma da DevStream combina funcionalidades essenciais, como controle de versão, pipelines de CI/CD, análise de vulnerabilidades e métricas de desempenho, em um único ambiente. Isso permite que empresas de diversos portes – desde startups ágeis até grandes corporações – acelerem a entrega de software com maior segurança e consistência. Além disso, a organização adota um modelo de negócios *open core* (versão básica como código aberto, enquanto funcionalidades avançadas são comercializadas).

2.1 Contexto

Tendências do Segmento (DevSecOps):

1. **Consolidação de Ferramentas**: Empresas buscam plataformas unificadas para reduzir complexidade e custos de integração. O GitLab se destaca ao oferecer uma única aplicação para todo o ciclo DevOps (desde planejamento até monitoramento).
2. **Segurança Integrada** (DevSecOps): A demanda por segurança embutida no pipeline de desenvolvimento cresce com ameaças cibernéticas. O GitLab incorpora varreduras de segurança, compliance e gestão de vulnerabilidades nativamente.
3. **Adoção de IA/ML**: Automação via IA para code review, sugestões de código e previsão de falhas é um diferencial. O GitLab já oferece features como Code Suggestions e planeja expandir soluções de IA generativa.

4. **Nuvem Híbrida e Multi-cloud**: Organizações adotam ambientes híbridos, exigindo flexibilidade. O GitLab suporta implantações em nuvem, self-managed e híbridas.
5. F**oco em Experiência do Desenvolvedor**: Redução de pontos de fricção no fluxo de trabalho (Diferentes linguagens, falta de conhecimento nas mesmas, etc). O GitLab investe em UX simplificada e integração contínua (CI/CD) eficiente.

Ambiente Competitivo:

1. Principais Concorrentes:

1. **GitHub (Microsoft)**: Domina em hospedagem de código, mas depende de integrações para CI/CD e segurança.
2. **Atlassian (Bitbucket/Jira)**: Forte em gestão de projetos, mas fragmentado em ferramentas (ex.: Bamboo para CI/CD).
3. **Provedores Cloud** (AWS, Azure, GCP): Oferecem serviços nativos (ex.: AWS CodePipeline), mas sem a integração end-to-end do GitLab.
4. **Especialistas em Segurança** (Snyk, SonarQube): Focados em nichos (apenas SAST/DAST), mas sem abrangência full-cycle.

2. Vantagem Competitiva do GitLab:

1. Plataforma Única: Elimina a necessidade de múltiplas ferramentas, reduzindo custos e falhas de integração.
2. Open Source + Enterprise: Atrai comunidades (GitLab CE) e empresas com recursos premium (GitLab EE).
3. Transparência Radical: Roadmap público e desenvolvimento colaborativo fortalecem a confiança de usuários.

3. Oportunidades:

1. Expansão em setores regulados (governo, saúde) com foco em compliance (ex.: FedRAMP, HIPAA).
2. Crescimento em mercados emergentes (Ásia-Pacífico, América Latina) com adoção acelerada de DevOps.
3. Parcerias estratégicas com provedores de nuvem e empresas de segurança.

4. Desafios:

1. Concorrência Agressiva: Gigantes como Microsoft e AWS investem pesado em suas soluções.
2. Complexidade de Escala: Manter a simplicidade enquanto adiciona funcionalidades avançadas.
3. Adoção Empresarial: Convencer grandes organizações a migrar de stacks fragmentados para uma plataforma única.

Conclusão:

O GitLab está bem posicionado com sua abordagem integrada de DevSecOps, alinhada às demandas por eficiência e segurança. Para manter a liderança, deve continuar inovando em IA, expandir presença global e reforçar parcerias estratégicas.

2.1.1 Missão - Fazer com que todos possam contribuir.

1. **Todos Podem Contribuir com o GitLab**: Ao oferecer ferramentas gratuitas e de código aberto (como GitLab CE/EE) e recursos de colaboração simplificados, eliminam barreiras para que qualquer pessoa proponha, construa e itere em software — a qualquer hora, em qualquer lugar — graças às práticas integradas de DevSecOps.

2. **Todos Podem Melhorar o GitLab, o Produto**: Cultivam uma comunidade global de contribuidores, acolhendo melhorias no aplicativo por meio de processos transparentes, iteração rápida e mentoria. Seus processos são baseados na ideia de 'merge requests' (análise de contribuição) em vez de consenso (Envolvimento desnecessário do time, reuniões demoradas e improdutivas, etc), permitindo que os usuários moldem as ferramentas que utilizam individualmente.

3. **Todos Podem Moldar o GitLab, a Empresa**: Por meio de práticas empresariais abertas, trabalho remoto e uma cultura de transparência, abrem a todo tipo de contribuição em seu 'handbook', as políticas e visão da empresa. As decisões seguem valores de eficiência, diversidade, e progresso orientado a resultados.

2.1.2 Valores - CREDIT

Valores do GitLab

A GitLab estrutura sua cultura em seis valores centrais **(CREDIT)**, que orientam comportamentos e decisões em todos os níveis da empresa. Cada valor é acompanhado por princípios operacionais concretos, visando alinhar ações e promover um ambiente colaborativo e eficiente.

1. Colaboração (C)

Prioriza o trabalho em equipe, ajuda mútua e feedback direto, com foco em separar críticas ao trabalho do respeito à pessoa. Incentiva a resolução de conflitos em ambientes privados (feedback negativo) e celebra contribuições publicamente.
Princípios incluem:

1. Sem ego: Decisões baseadas em méritos, não em hierarquia.
2. Assumir boa-fé: Evitar julgamentos precipitados e promover diálogo aberto.
3. Aceitar contribuições de qualquer pessoa, sem territorialismo.

2. Resultados para Clientes (R)

1. O valor supremo na hierarquia, direcionando tudo para o sucesso do cliente. Princípios-chave:
2. Cocriação: Desenvolver soluções junto aos clientes e escalá-las globalmente.
3. Foco no usuário final: Evitar o "Efeito Concur" (complexidade desnecessária).
4. Impacto superior à atividade: Medir resultados, não horas trabalhadas.

3. Eficiência (E)

1. Otimiza processos globalmente, priorizando simplicidade e redução de desperdícios:
2. Soluções "chatas": Usar tecnologias consolidadas, não inovações por modismo.
3. Autosserviço: Documentar tudo para evitar dependência.
4. Gerenciamento do próprio tempo: Reuniões só quando necessárias, com agendas claras.

4. Diversidade, Inclusão e Pertencimento (D)

1. Promove um ambiente seguro e acolhedor para todas as origens:
2. Comunicação assíncrona: Respeitar fusos horários e responsabilidades pessoais.
3. Combate a micro agressões: Conscientização sobre impactos sutis de palavras e ações.
4. "Contratação por contribuição cultural": Valorizar diferenças, não homogeneidade.

5. Iteração (I)

1. Valoriza progresso incremental com feedback rápido:
2. Mudança Mínima Valiosa (MVC): Entregar a versão mais simples funcional e aprimorar gradualmente.
3. "Não espere": agir rapidamente, evitando perfeccionismo paralisante.
4. Decisões reversíveis: priorizar ações de baixo risco para acelerar o aprendizado.

6. Transparência (T)

1. Informações públicas por padrão, exceto quando legalmente sensíveis:
2. Documentação aberta: Handbook, issues e decisões acessíveis a todos.
3. Diretividade: Comunicação clara e honesta, mesmo em erros.

4. Fonte única da verdade: centralizar dados para evitar ambiguidades.

Manutenção dos Valores

1. A GitLab integra seus valores em processos críticos:
2. Contratações e promoções: avaliação alinhada aos valores.
3. Feedback 360°: comportamentos são revisados em avaliações anuais.
4. Exemplo da liderança: O E-group modela valores em decisões e comunicações.

Hierarquia em Conflitos:

Quando valores colidem, a prioridade é:

1. Resultados para Clientes
2. Colaboração
3. Transparência
4. Iteração
5. Eficiência
6. Diversidade, Inclusão e Pertencimento

A empresa evita politização interna, incentivando meritocracia e decisões baseadas em dados. Valores são dinâmicos, revisados constantemente via contribuições coletivas, refletindo o compromisso da GitLab com evolução contínua e inclusão global.

A GitLab visa entregar, nos próximos 10 anos, soluções inovadoras alinhadas à sua missão de 30 anos e estratégia corporativa de 3 anos. **Sua abordagem inclui**:

Adaptação ao Mercado:

1. Monitora mudanças e integra novas tecnologias (ex.: controle de versão futuro) para manter sua plataforma DevSecOps aberta e relevante.
2. Aprende com exemplos como a Netflix, que priorizou timing estratégico para transições de mercado.

Expansão em Novos Mercados:

1. **Consolidação de Categorias:** Unifica ferramentas fragmentadas (ex.: SCM + CI) em fluxos integrados, reduzindo custos e permitindo contribuição direta dos usuários.
2. **Criação de Categorias:** Gera novos mercados (ex.: cadeia de ferramentas unificadas) com alto potencial de crescimento (CAGR), alinhando ciclos de adoção de tecnologia para sustentar expansão orgânica.

Objetivo Final:

Tornar seu modelo de consolidação/criação de mercados quantificável e sistemático, facilitando a avaliação ágil de oportunidades e garantindo crescimento sustentável.

2.2 O negócio

- A organização opera no segmento de plataformas integradas de DevOps, focada em desenvolvimento, entrega e segurança de software.
- Atende empresas de diversos portes (startups, PMEs (Pequenas e Médias empresas), e setores, com soluções adaptáveis a necessidades específicas.
- Oferece serviços via modelo SaaS (nuvem) ou implantação em ambientes autogerenciados, garantindo flexibilidade e conformidade com regulamentações.
- Plataforma unificada de DevOps: Controle de versão, integração contínua (CI/CD), gerenciamento de segurança e monitoramento de desempenho em um único ambiente
- Modelo Open Core: Versão básica gratuita e de código aberto, fomentando a colaboração da comunidade em seu desenvolvimento, com licenças premium para funcionalidades avançadas (ex., segurança empresarial, auditoria de conformidade).
- Serviços Complementares: Consultoria para implementação de práticas DevOps, Treinamentos técnicos e certificações em uso da plataforma, suporte prioritário para correção de falhas e otimização de fluxos.
- Venda de Soluções Especializadas: Ferramentas de segurança integradas ao ciclo de desenvolvimento (ex., varredura de vulnerabilidades em tempo real 'SAST', 'DAST' ou 'Secret Detection') e módulos para gerenciamento ágil de projetos, como quadros Kanban e rastreamento de issues.
- Integração com Ecossistemas Externos: Conectores para nuvens públicas (AWS, Google Cloud), ferramentas de monitoramento (Prometheus) e sistemas de autenticação.
- Atua globalmente, com equipe 100% remota e suporte multilíngue.

3 Os principais processos de negócios

3.1 Fluxograma do Pipeline de CI/CD Seguro

> Commit de Código (Branch Feature)

O desenvolvedor realiza commit de código em uma branch de feature no sistema de controle de versão (ex: Git). Por exemplo, um desenvolvedor corrige um bug na funcionalidade de login e faz o commit das alterações na branch feature/login-fix. A integração com ferramentas de versionamento do GitLab são cruciais para este passo.

> Disparo da Pipeline (via Git Push/Merge Request)

O commit ou merge request dispara automaticamente a pipeline de CI/CD.
Configuração de triggers no sistema de CI/CD é essencial. Métricas como tempo médio de resposta ao commit (ex: < 5 segundos) podem ser monitoradas.

> Execução de Jobs (Build, Test, Scan)

A Execução de Jobs abrange Build, Test e Scan para garantir a qualidade e segurança do código. O Build gera artefatos executáveis, o Test executa testes automatizados e o Scan identifica vulnerabilidades. Além disso, a Verificação de Credenciais (Secret Detection) detecta credenciais expostas no código, interrompendo a pipeline caso necessário.

> Artefatos Gerados (Binários, Logs)

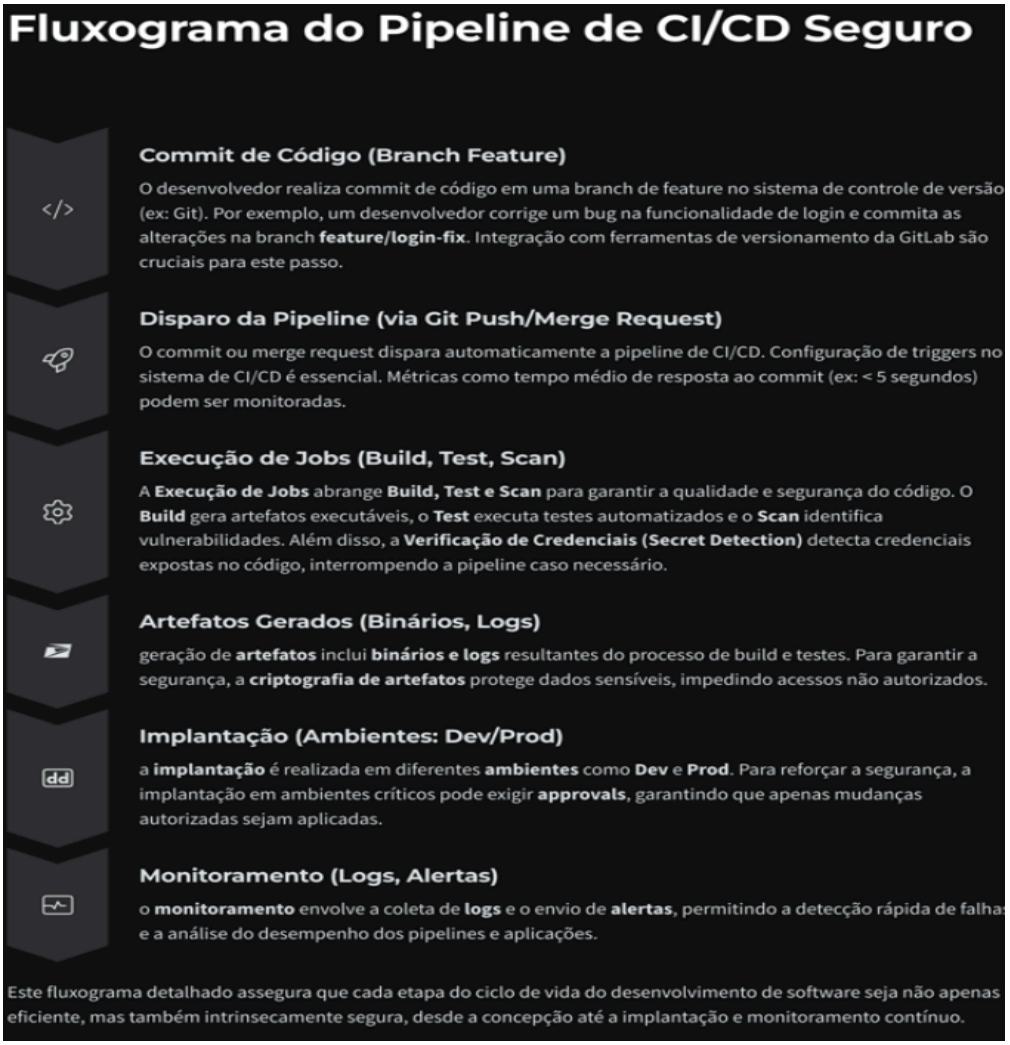
A geração de artefatos inclui binários e logs resultantes do processo de build e testes. Para garantir a segurança, a criptografia de artefatos protege dados sensíveis, impedindo acessos não autorizados.

> Implantação (Ambientes: Dev/Prod)

A implantação é realizada em diferentes ambientes como Dev e Prod. Para reforçar a segurança, a implantação em ambientes críticos pode exigir approvals, garantindo que apenas mudanças autorizadas sejam aplicadas.

> Monitoramento (Logs, Alertas)

O monitoramento envolve a coleta de logs e o envio de alertas, permitindo a detecção rápida de falhas e a análise do desempenho dos pipelines e aplicações.



3.2 Fluxograma de Gestão de Repositórios

> Criação do repositório (Privado/Público)

Defina o tipo de repositório (privado ou público).
Implemente políticas de nomenclatura consistentes.

> Configuração inicial (Branches protegidos, Permissões RBAC)

Defina branches protegidos para evitar commits diretos.
Implemente controle de acesso baseado em roles (RBAC).

> Desenvolvimento (Commits, Branches)

Crie branches de feature para desenvolvimento isolado. O desenvolvimento envolve a criação de commits e branches para organizar o código. Para garantir a segurança, são realizadas verificações de segredos através de: SAST (Static Application Security Testing) e DAST (Dynamic Application Security Testing). Esses testes identificam vulnerabilidades e segredos expostos no código.

> Merge Request (Revisão, Approvals)

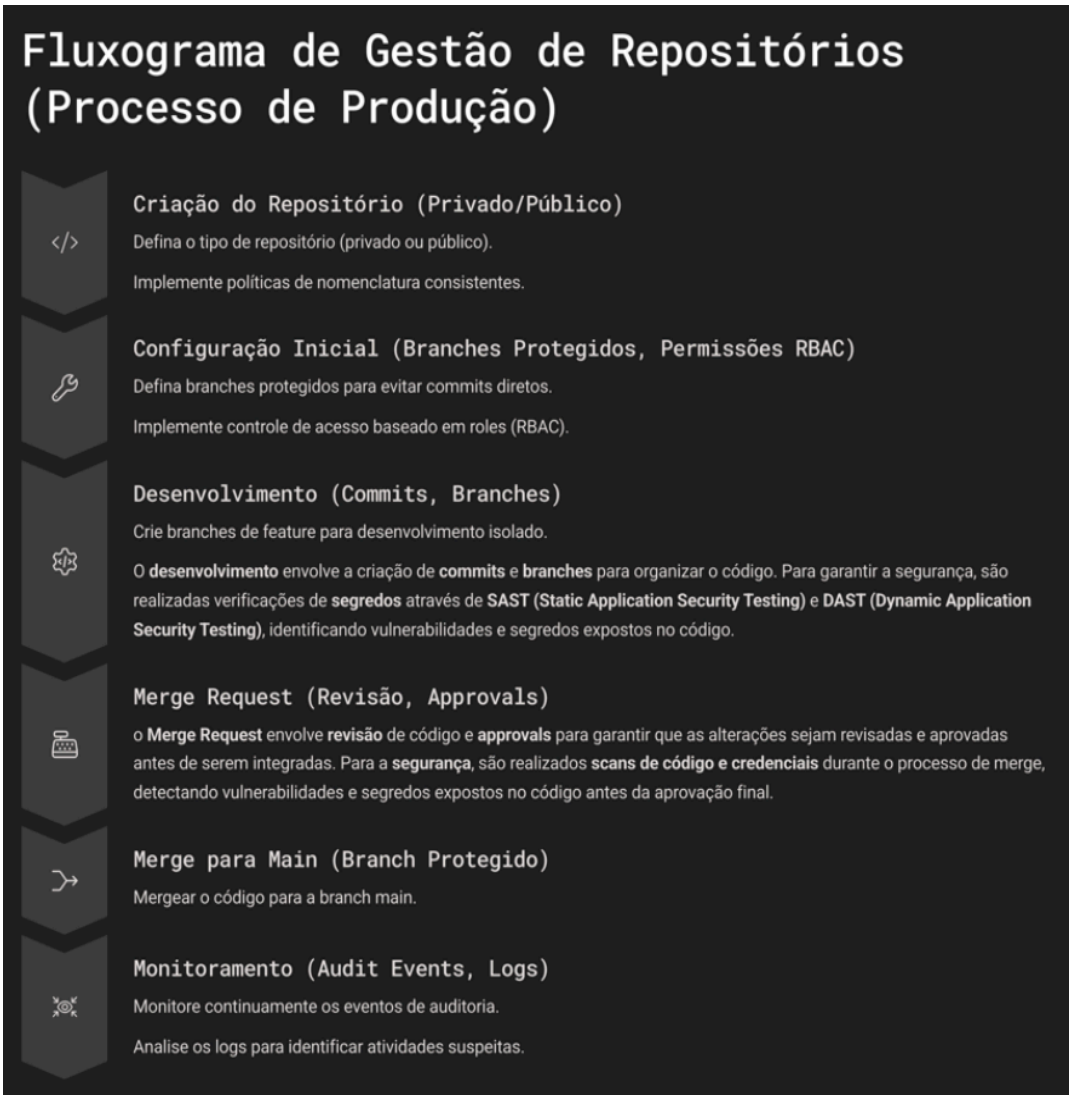
O Merge Request envolve revisão de código e approvals para garantir que as alterações sejam revisadas e aprovadas antes de serem integradas. Para segurança, são realizados scans de código e credenciais durante o processo de merge, detectando vulnerabilidades e segredos expostos no código antes da aprovação final.

> Merge para Main (Branch Protegido)

Mergear o código para a branch main.

> Monitoramento (Audits, Events, Logs)

Monitore continuamente os eventos de auditoria e analise os logs para identificar atividades suspeitas.



4 Leis relacionadas a TI que impactam o negócio

Lei	Impacto na organização
LGPD (Lei Geral de Proteção de Dados - Lei nº 13.709/2018)	- Controle de acesso de usuários: apenas equipes autorizadas devem manipular dados pessoais. - Implantação de políticas de privacidade e consentimento. - Criação de mecanismos para exclusão, anonimização e rastreamento de dados.
Marco Civil da Internet (Lei nº 12.965/2014)	- Obrigatoriedade de manter registros de acesso por um período determinado. - Garantia da neutralidade da rede e da privacidade dos usuários. - Estabelece responsabilidade civil por danos gerados por terceiros em ambiente digital.

Lei de Crimes Cibernéticos (Lei nº 12.737/2012)	- Reforço nas políticas de segurança da informação. - Prevenção e mitigação de ataques cibernéticos, como invasões, roubo de dados e fraudes.
Lei de Acesso à Informação (Lei nº 12.527/2011)	- Aplicável a organizações públicas ou prestadoras de serviço público. - Garante a transparência ativa e passiva de dados institucionais e obriga cuidados no compartilhamento.

Matriz de relacionamento de processos organizacionais e leis.

Processo	**Leis relacionadas**	**Observações**
Gerenciamento de relacionamento de cliente	LGPD	Garantir o consentimento para uso de dados, transparência e segurança no tratamento das informações.
Gestão de TI e infraestrutura	Lei de Crimes Cibernéticos, Marco Civil	Garantir uso legal de software, segurança contra ataques, e guarda de logs de acesso conforme exigido.
Transparência e compliance	Lei de Acesso à Informação, LGPD	Divulgar informações obrigatórias e assegurar o cumprimento das normativas de privacidade e segurança.

5 Referências

GITLAB. Company mission. *GitLab Handbook*]. Disponível em: https://handbook.gitlab.com/handbook/company/mission/. Acesso em: 24 mar. 2025.

GITLAB. Company vision. *GitLab Handbook*. Disponível em: https://handbook.gitlab.com/handbook/company/vision/. Acesso em: 24 mar. 2025.

GITLAB. Company strategy. *GitLab Handbook*. Disponível em: https://handbook.gitlab.com/handbook/company/strategy/. Acesso em: 24 mar. 2025.

GITLAB. GitLab values. *GitLab Handbook*. Disponível em: https://handbook.gitlab.com/handbook/values/. Acesso em: 24 mar. 2025.

GitLab Inc. (2025). *Sobre o GitLab*. GitLab. Disponível em: https://about.gitlab.com

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 24 mar. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. *Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet)*. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 24 mar. 2025.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. *Dispõe sobre a tipificação criminal de delitos informáticos (Lei Carolina Dieckmann)*. Diário Oficial da União: seção 1, Brasília, DF, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 24 mar. 2025.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. *Regula o acesso a informações previsto na Constituição Federal (Lei de Acesso à Informação)*. Diário Oficial da União: seção 1, Brasília, DF, 18 nov. 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 24 mar. 2025.