

A thick black L-shaped frame is positioned on the left and bottom edges of the slide, framing the central text.

# ASPECTOS LEGAIS E REGULAMENTARES

Auditoria de Software e Proteção de Dados

# Objetivo da Aula

- Entender os principais aspectos legais e regulatórios relacionados à auditoria de software, com foco na LGPD e GDPR.
- Discutir como a conformidade com essas regulamentações afeta a auditoria de software.
- Conhecer penalidades e exemplos reais de não conformidade.
- Explorar processos de auditoria que asseguram o cumprimento das leis.

# Introdução às Normas de Proteção de Dados

- LGPD (Lei Geral de Proteção de Dados)
  - *Regula o tratamento de dados pessoais no Brasil.*
  - *Direitos: consentimento, acesso, retificação, portabilidade e exclusão.*
  - *Empresas devem garantir segurança e privacidade dos dados.*
- GDPR (General Data Protection Regulation)
  - *Regula o uso de dados pessoais na União Europeia.*
  - *Direitos: acesso, esquecimento, portabilidade e limitação de tratamento.*
  - *Auditorias são obrigatórias para demonstrar conformidade.*

# Impacto das Normas na Auditoria de Software

- A auditoria verifica se as empresas cumprem as normas de proteção de dados.
- Avalia medidas técnicas e administrativas implementadas.
- Exemplo de verificação:
  - *Criptografia e anonimização de dados sensíveis.*
  - *Controles de acesso e autenticação de usuários.*
  - *Registro de logs e incidentes de segurança.*
  - *Planos de resposta e notificação de vazamentos.*

# Casos Reais: LGPD no Brasil

- Serasa Experian (2021)
  - *Vazamento de dados de mais de 220 milhões de brasileiros.*
  - *Multa e exigência de revisão das políticas de segurança.*
  
- Banco Pan (2023)
  - *Penalidade aplicada após falha de segurança expor dados de clientes.*
  - *Auditoria determinou falta de controle de acesso adequado.*
  
- iFood (2022)
  - *Dados de clientes e entregadores vazaram após acesso indevido.*
  - *Empresa implementou auditorias internas periódicas.*

# Casos Reais: GDPR na Europa

- Meta (Facebook) – Irlanda, 2023
  - *Multa de €1,2 bilhão por transferência ilegal de dados para os EUA.*
- Google – França, 2020
  - *Multa de €50 milhões por falta de transparência e consentimento claro.*
- British Airways – Reino Unido, 2019
  - *Multa de £20 milhões após violação de dados de 400 mil clientes.*
- Amazon – Luxemburgo, 2021
  - *Multa de €746 milhões por descumprimento de regras de consentimento.*

# Penalidades por Não Conformidade

- LGPD:

- *- Multas de até 2% do faturamento da empresa (limite: R\$ 50 milhões por infração).*

- GDPR:

- *Multas de até 4% do faturamento global anual ou 20 milhões de euros.*

- Além das multas:

- *Danos à reputação da marca.*
  - *Perda de confiança dos clientes.*
  - *Interdição de tratamento de dados.*

# Exemplo de Processo de Auditoria

- 1. Planejamento da auditoria e definição do escopo.
- 2. Levantamento de políticas e controles de segurança.
- 3. Testes e validações de proteção de dados.
- 4. Elaboração de relatório com recomendações.
- 5. Acompanhamento da implementação das melhorias.



# Boas Práticas e Conclusão

- Promover treinamentos sobre proteção de dados.
- Implementar políticas de privacidade claras e acessíveis.
- Realizar auditorias periódicas e testes de segurança.
- Registrar e documentar todas as ações de conformidade.
- A auditoria de software é essencial para garantir a proteção e a confiança digital.