THE DEVELOPER'S CONFERENCE

Software Security

Privacidade por Desenho

Luiz Eduardo Gava

LGPD

THE DEVELOPER'S CONFERENCE

- Lei Geral de Proteção de Dados pessoais
  - Aprovada em Julho/2018
  - Prazo para adaptação até Agosto/2020

MAIS REQUISITOS!

A LGPD em três slides

THE DEVELOPER'S CONFERENCE

- Dados Pessoais = Informação relacionada a pessoa natural identificada ou identificável.

10 Bases Legais

THE DEVELOPER'S CONFERENCE

- Obrigação Legal, Políticas Públicas, Pesquisas, Contratos, Processos, Proteção da Vida, Saúde, Proteção do Crédito
- Interesses Legítimos
- Consentimento

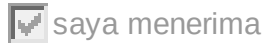
Consentimento

THE DEVELOPER'S CONFERENCE

- Manifestação livre
- Informado
- Inequívoco
- Específico para determinada finalidade
- Atualizado
- Revogável

Termo de Uso

Este conteúdo tem propósitos educacionais apenas. Ceci n'est pas une pipe. Qualquer semelhança com pessoas reais, vivas ou não, físicas ou jurídicas, naturais ou sobrenaturais, é mera coincidência. Pilhas não estão incluídas. Não sou advogado, busque aconselhamento profissional. Os veículos neste estacionamento não estão cobertos por nenhum tipo de seguro. Sua privacidade não tem nenhum valor. Estes slides não representam a opinião do autor, nem de sua empresa, de seus amigos ou de seu cão. Estes termos estão sujeitos a mudanças a qualquer momento, sem avisos. Nenhum animal foi maltratado durante a elaboração destes slides. Usar em ambiente arejado. Não fazemos trocas nem devoluções. Para uso recreacional apenas. Outras restrições se aplicam. Não recomendado para menores de idade. O usuário abre mão de todos os seus direitos e aceita entregar sua alma e dados pessoais ao demônio ou a qualquer terceiro. Conteúdo fornecido sem garantias. É reservado o direito de suspender, encerrar, modificar ou excluir sua conta a qualquer momento, sem qualquer responsabilidade com você até o limite da lei aplicável. Qualquer reprodução, redistribuição e modificação dessas propriedades é proibido por esse contrato. Você concorda em indenizar, defender e isentar o autor contra todas e quaisquer reivindicações, ações jurídicas, danos, perdas, responsabilidades e despesas (incluindo honorários) em qualquer situação. Se você aceita esses termos, não clique aqui. Marcar a caixa significa aceitação completa e irrestrita de todos os termos, mesmo que você não os tenha lido.



Privacidade

THE DEVELOPER'S CONFERENCE

O que é privacidade ???

- Privacidade = controle, autodeterminação informativa
- Privacidade ↔ Liberdade
- Privacidade → Segurança da Informação + Ética

Abusos de Privacidade

THE DEVELOPER'S CONFERENCE

- Organização pode fazer mal uso dos dados pessoais.
- Funcionários da organização podem cometer abusos.
- Outros podem roubar dados desprotegidos.
- Um governo pode obter os dados, discriminar e prender pessoas (como durante a 2ª Guerra Mundial)

Privacidade por Desenho

THE DEVELOPER'S CONFERENCE

- Conceito pela Dra. Ann Cavoukian (1995)
- Publicação do framework (2008)
- OWASP Top 10 Privacy Risks (2014)
- GDPR Artigo 25 (2018)
- ISO está preparando um novo padrão (ISO 31700)

Privacidade por Desenho

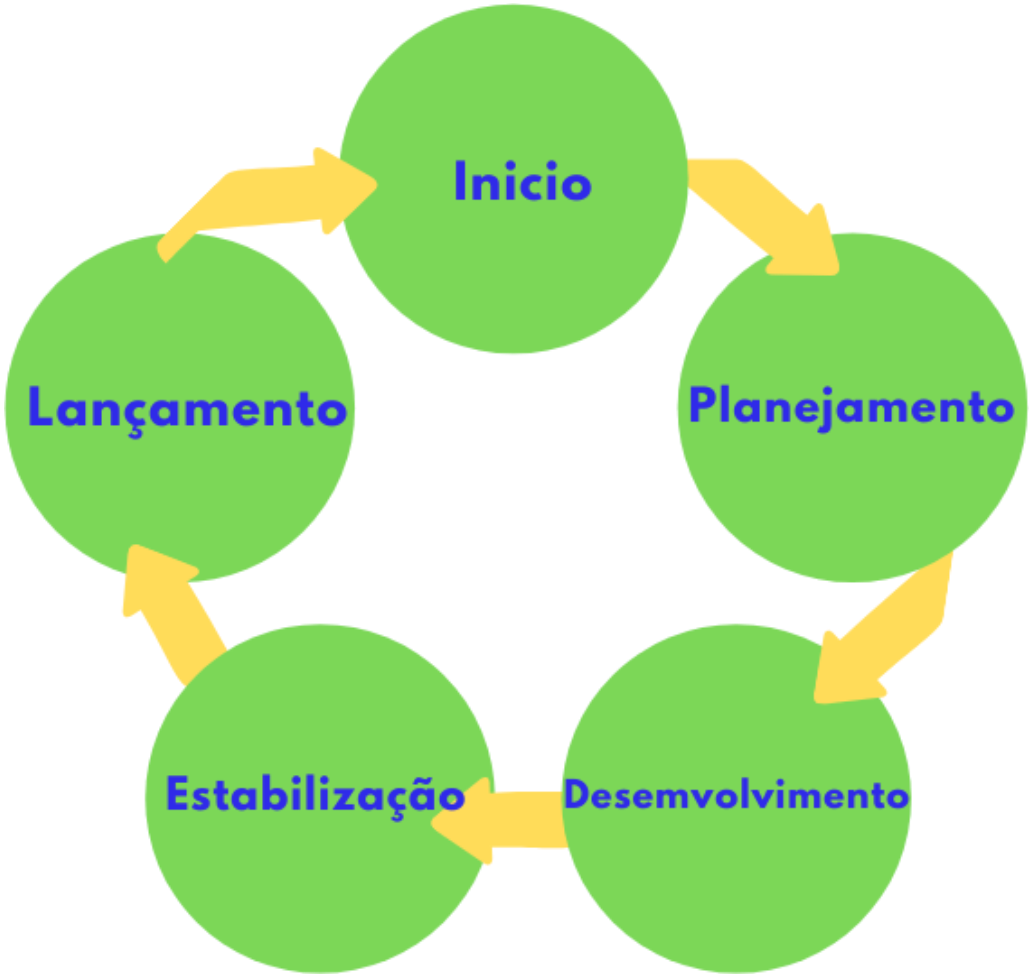
Privacidade por Desenho é uma metodologia na qual a proteção de dados pessoais é pensada desde a concepção de sistemas, processos, práticas comerciais, projetos, produtos ou qualquer outra solução que envolva o manuseio de dados pessoais.

7 Princípios Básicos

THE DEVELOPER'S CONFERENCE

- Proatividade: prevenir é melhor do que remediar
- Privacidade como padrão
- Privacidade no desenho
- Funcionalidade total: soma positiva
- Segurança de ponta a ponta
- Visibilidade e Transparência
- Respeito à Privacidade

Ciclo de Desenvolvimento



Inicio

THE DEVELOPER'S CONFERENCE

- Identificar os requisitos de dados pessoais, Segurança e Privacidade
- Engajar equipes de Segurança e Privacidade

Planejamento

THE DEVELOPER'S CONFERENCE

- Identificar o propósito de cada dado coletado
- Classificação dos dados
- Retenção dos dados
- Análise de Impacto à Privacidade (DPIA)
- Registrar dados em CMDB, identificar fluxos

Desenvolvimento

THE DEVELOPER'S CONFERENCE

- Incluir classificação e retenção dos dados no modelo de dados
- Consentimento, onde necessário
- Criptografia de dados em transito ou armazenados
- Direitos do Titular de Dados Pessoais
- Integridade de Dados
- Autenticação e Autorização
- Análise de Segurança de Código

Estabilização

THE DEVELOPER'S CONFERENCE

- Pen test

THE DEVELOPER'S CONFERENCE

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

— Edward Snowden

THE DEVELOPER'S CONFERENCE

POASEC.org

Disseminando segurança, criando cultura.

LGPD

tecnologia a serviço da cidade

procempa

Luiz Eduardo Gava

luiz.gava@poasec.org

OWASP

Open Web Application Security Project

THE DEVELOPER'S CONFERENCE