A regulamentação LGPD

e as implicações práticas nas empresas brasileiras

Agenda

- **Contexto**
- Conceitos inerentes à LGPD
- Aspectos técnicos e legais da LGPD
- Como implementar (na prática) os mecanismos de controle e compliance
- Treinamentos e certificações
- Considerações finais

Contexto

- A “Era da Informação”
  - Rápida adoção da tecnologia por todos
  - Falta de maior preocupação com a segurança
  - Escopo internacional
- A “ética *hacker*” original não resistiu ao temp
  - Já existem mais de 30.000 sites orientados a *hacke*
  - Não é mais necessários ser um “nerd” ou um guru da tecnologia
  - *Hacktivismo* como protesto político e/ou social (Grupo Anonymous)

Contexto

- Motivação para o *hacking x* Impacto ao usuário
  - Até 2000 - **Prova de Conhecimento**: *Phishing* (*I was here*)
  - De 2001 à 2010 - **Destruição da informação**: *Malwares* (sites/sistemas fora do ar)
  - De 2010 à 2015 - **Indisponibilização da informação**: *DDOS* (sites fora do ar)
  - De 2015 à 2018 - **Sequestro da informação**: Ransomware (sistemas fora do ar)
  - Atualmente - **Uso da informação**: Cambridge Analytica (“nada” fora do ar)
    - Dados dos usuários do Facebook ► Eleição Americana
    - Qual o impacto para o usuário???

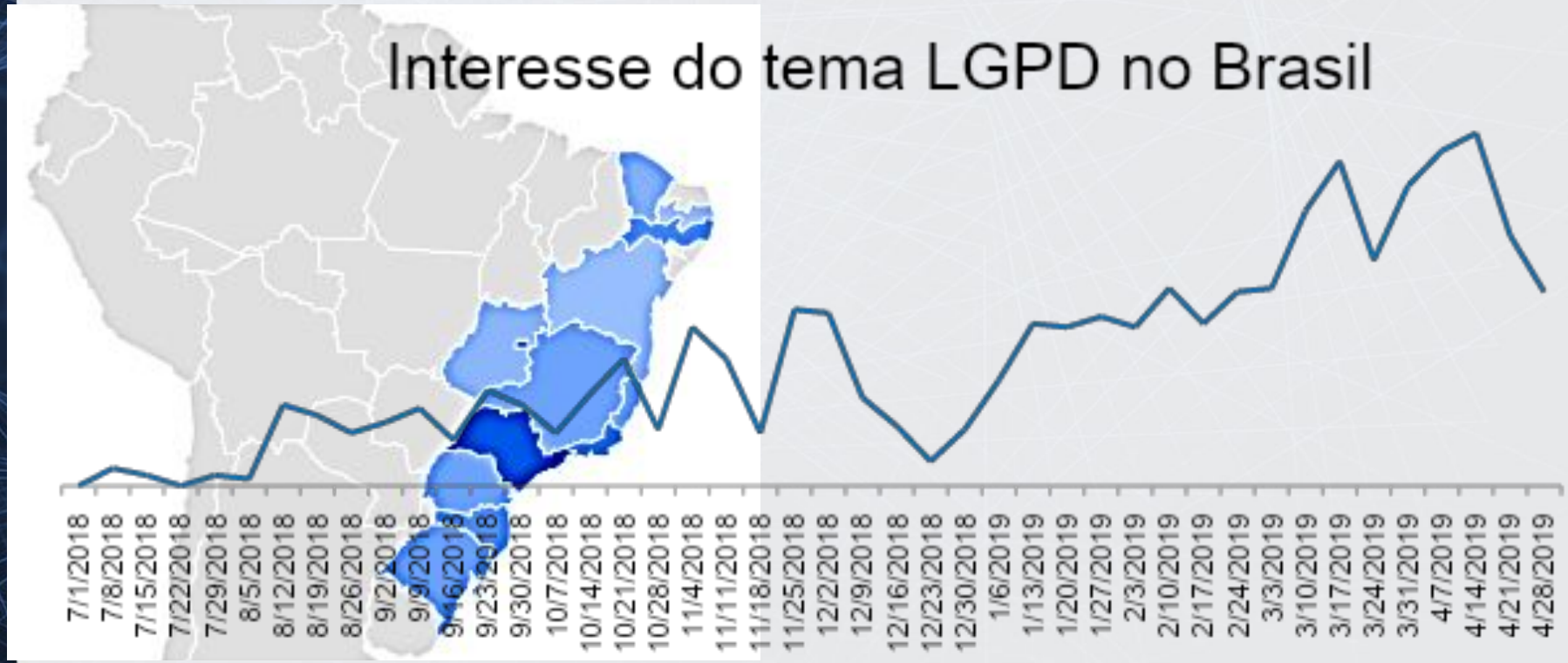
Contexto

- GDPR (*General Data Protection Regulation*)
  - Estudos e normativas iniciais desde 1995
  - Adota na Europa em abril de 2016
  - Entrada em vigor em maio de 2018
  - Objetivo principal é garantir a privacidade do **cidadão** europeu
  - Penalizações que podem chegar a 4% do faturamento da empresa (restrita a 20Mi €)
  - Extensível a todos os países que fazem comércio com a Europa

Contexto

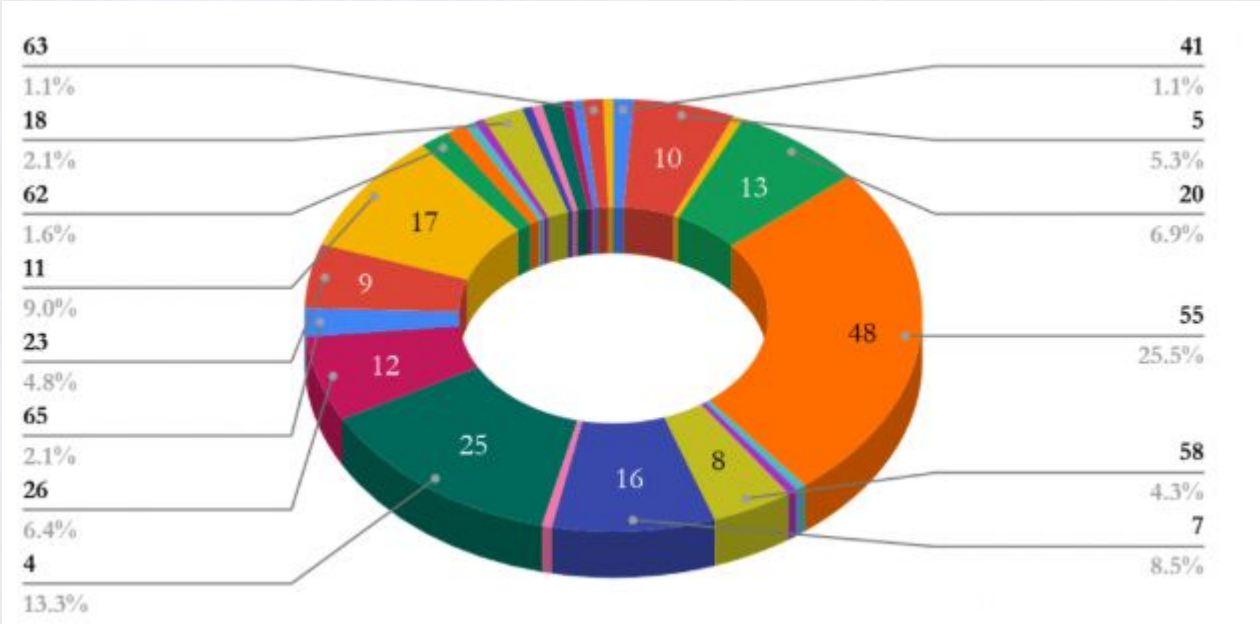
- LGPD (Lei Geral de Proteção de Dados)
  - Lei nº 13.709/18
  - Promulgada em 14/08/2018
  - Criação da ANPD em 28/12/2018 (M. P. nº 869)
  - Passa a vigorar a partir de Agosto/2020
  - Penalizações que podem chegar a 2% do faturamento da empresa (restrita a R$50Mi)

Contexto


Interesse do tema LGPD no Brasil
7/1/2018
7/8/2018
7/15/2018
7/22/2018
7/29/2018
8/5/2018
8/12/2018
8/19/2018
8/26/2018
9/2/2018
9/9/2018
9/16/2018
9/23/2018
9/30/2018
10/7/2018
10/14/2018
10/21/2018
10/28/2018
11/4/2018
11/11/2018
11/18/2018
11/25/2018
12/2/2018
12/9/2018
12/16/2018
12/23/2018
12/30/2018
1/6/2019
1/13/2019
1/20/2019
1/27/2019
2/3/2019
2/10/2019
2/17/2019
2/24/2019
3/3/2019
3/10/2019
3/17/2019
3/24/2019
3/31/2019
4/7/2019
4/14/2019
4/21/2019
4/28/2019

Contexto

- Número de propostas de emenda por artigo da LGPD: Total **176** (???)



Agenda

- Contexto
- **Conceitos inerentes à LGPD**
- Aspectos técnicos e legais da LGPD
- Como implementar (na prática) os mecanismos de controle e compliance
- Treinamentos e certificações
- Considerações finais

Conceitos inerentes à LGPD

- **Dados pessoais**: qualquer informação relativa a uma pessoa singular identificada ou identificável (Art. 4º da G.D.P.R. de 2006)
  - Dados diretos: podem ser atribuídos a um dado específico sem o uso de informações adicionais (DNA, digital, foto, etc.)
  - Dados indiretos: não podem ser atribuídos a um indivíduo de dados específicos sem o uso de informações adicionais (IP, placa do carro, etc.)

  - Dados pseudonimizados: dados pessoais processados e não podem mais ser atribuídos ao titular de dados, mas o processo ainda pode ser revertido (com uma chave)
  - **Anonimização: a pessoa a quem os dados se refere não pode mais ser identificada**

Conceitos inerentes à LGPD

- **Dados sensíveis**: categoriais especiais de dados pessoais (Art. 9º §10)
  - Origem racial ou étnica
  - Opiniões políticas
  - Dados genéticos
  - Dados relativos à saúde
  - Crenças religiosas, filosóficas ou filiação sindical
  - Dados biométricos com o propósito de identificar unicamente uma pessoa
  - Dados relativos à vida sexual ou orientação sexual de uma pessoa singular

Conceitos inerentes à LGPD

- **Controlador** (*data controller*): pessoa natural ou jurídica, de direito público ou privado, a quem compete as **decisões** referente ao tratamentos dos dados
- **Operador** (*data processor*): pessoa natural ou jurídica, de direito público ou privado, a que realiza o **tratamento** dos dados em nome do controlador
- **Oficial** (DPO - *data protection officer*): profissional (interno ou externo) para a proteção dos dados e **responsável pelo cumprimento** da lei

Agenda

- Contexto
- Conceitos inerentes à LGPD
- **Aspectos técnicos e legais da LGPD**
- Como implementar (na prática) os mecanismos de controle e compliance
- Treinamentos e certificações
- Considerações finais

Aspectos técnicos e legais da LGPD

- Aspectos técnicos
  - Redes e arquitetura *cloud*
  - Técnicas de encriptação e segurança da informaçã
  - Códigos fontes
  - Técnicas de anonimização de dados e *data maskir*
  - Compreensão da arquitetura de infraestrutura
  - Compreensão da arquitetura de sistemas (bases d

Aspectos técnicos e legais da LGPD

- Aspectos legais
  - Implementação de políticas de segurança da info
  - Implementação de políticas de privacidade
  - Modelos de gestão baseados em privacidade
  - Definição de códigos de ética
  - *Cyber insurance* (seguro)

Agenda

- Contexto
- Conceitos inerentes à LGPD
- Aspectos técnicos e legais da LGPD
- **Como implementar (na prática) os mecanismos de controle e compliance**
- Treinamentos e certificações
- Considerações finais

Como implementar (na prática) os mecanismos de controle e compliance

R$4Bi
Faturamento

4,5Mi
Litros/dia

2.600
Colaboradores

5
Fábricas
(GO/MG/SC/RS/PR)

140
Produtos

Como implementar (na prática) os mecanismos de controle e compliance

- Motivações da **jornada** LGPD na sua empresa
  - Estratégia corporativa: comece na frente... tenha um diferencial (case Santander)
  - Gestão de contratos: garanta a proteção de dados fim-a-fim
  - PCN (Plano de Continuidade de Negócios): CAPEX x OPEX

Como implementar (na prática) os mecanismos de controle e compliance

- Metodologia (???) de implantação
  - Definir rapidamente (mas com critérios) o DPO: Jurídico ou TI?
  - Análise de negócio: qual a área de atuação da empresa?
  - Análise de requisitos da LGPD: FIT x GAP
    - Validação dos requisitos de TI: base de dados de **todos** os sistemas
    - Validação dos requisitos jurídicos: contratos pessoais (RH) e corporativos (fornecedores)
  - Análise da matriz DPIA: qual o risco para a empresa?

Como implementar (na prática) os mecanismos de controle e compliance

- Passo-a-passo (???) para implantação

1. Readequar processos internos de tratamentos dos dados (mudança de cultura)
2. Revisar as políticas de privacidade (internas e externas)
3. Revisar os contratos que impliquem em processamento de dados (*data processors*)
4. Revisar as bases legais de tratamento: consentimento, legítimo interesse
5. Implementar o registro de processamento de dados
6. Revisar a política de incidentes de dados para garantir resposta à A.N.P.D.

Como implementar (na prática) os mecanismos de controle e compliance

Engajamento

- Atuar de forma interdisciplinar
- Participe das entidades no assunto

Planejamento

- É uma jornada.. não um projeto
- Cuidado com as armadilhas dos detalhes

Execução

- Esteja preparado para mudanças
- Foco, FOCO na LGPD
- Treine toda a empresa

PDCA

- Atue rapidamente
- Considere apoio externo
- Treine (**sempre**) toda a empresa

Agenda

- Contexto
- Conceitos inerentes à LGPD
- Aspectos técnicos e legais da LGPD
- Como implementar (na prática) os mecanismos de controle e compliance
- **Treinamentos e certificações**
- Considerações finais

Treinamentos e certificações

- Jornada “oficial” Exin
  - ISO27001
  - PDPF: *Privacy & Data Protection Foundation*
  - PDPP: *Privacy & Data Protection Practitioner*

- Outras instituições
  - Assespro RS
  - Escola Virtual: www.escolavirtual.gov.br/curso/153

Agenda

- Contexto
- Conceitos inerentes à LGPD
- Aspectos técnicos e legais da LGPD
- Como implementar (na prática) os mecanismos de controle e compliance
- Treinamentos e certificações
- **Considerações finais**

Considerações finais

- Lembre-se: a lei se aplica a empresas/site **dentro e fora** do país
- A.N.P.D. não tem orçamento: aplicações de sansões e **multas**
- Consentimento: menores de 16 anos **não podem** consentir o uso de dados
- Nunca subestime o interesse alheio: Tr3v0r - case SUS (200Mi de usuários)

- Busque informações em locais “seguros”
- Desconfie de “soluções mágicas” de fornecedores
- Comece sua jornada **HOJE**!

A regulamentação LGPD

e as implicações práticas nas empresas brasileiras

OBRIGADO!

Rogério Mendes

www.linkedin.com/in/rmendesferreira