

RISCOS DO TRATAMENTO DE DADOS & ARQUITETURA DE SEGURANÇA DA INFORMAÇÃO

LIÇÕES EXTRAÍDAS DE GRANDES
VAZAMENTOS DE DADOS



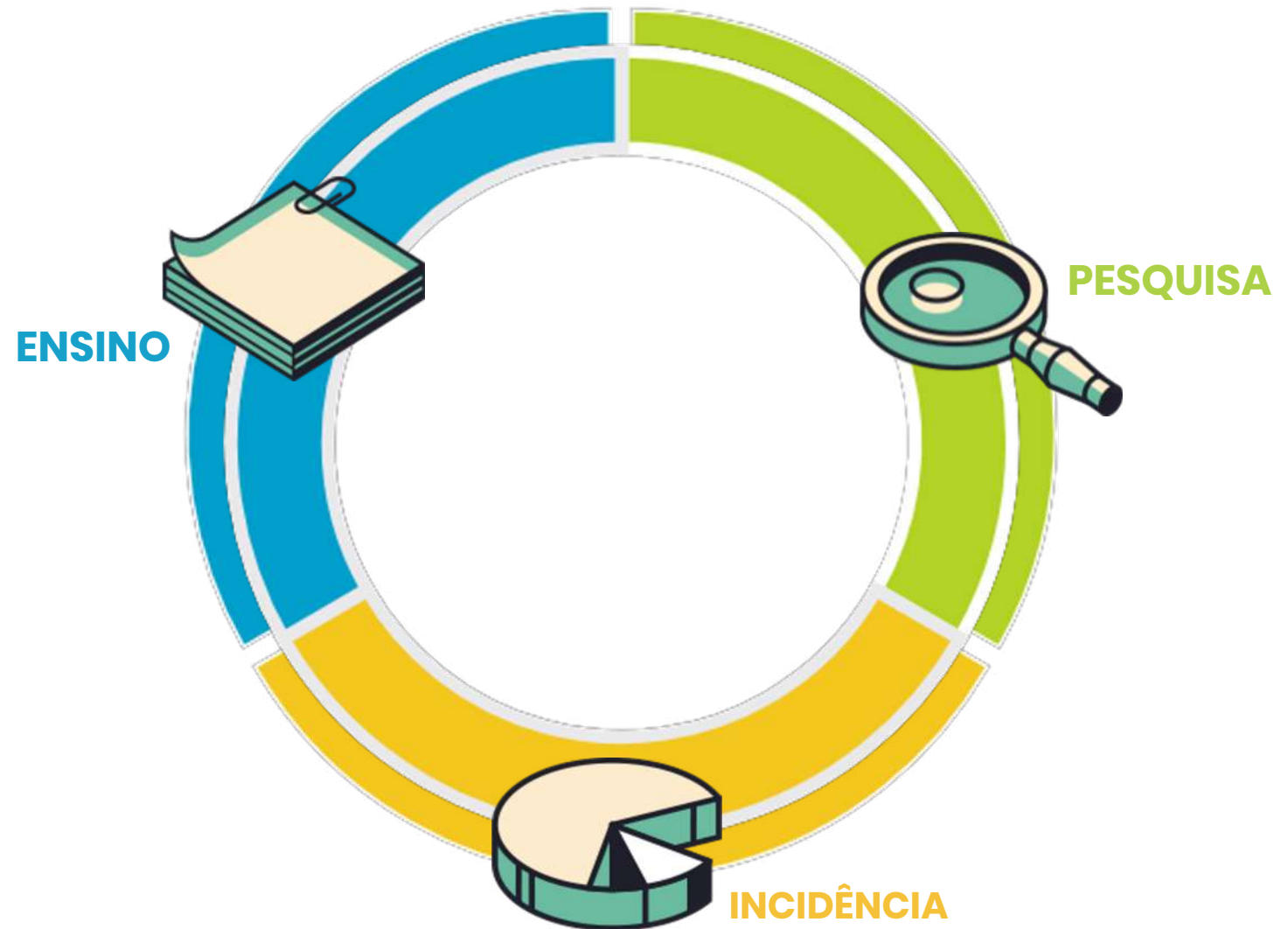
DataPrivacyBR
RESEARCH



QUEM SOMOS

.....
.....
.....

Espaço de articulação entre
duas organizações distintas e
complementares:
**Data Privacy Ensino e Data
Privacy Pesquisa**







AGENDA

1. RISCO E PROTEÇÃO DE DADOS
2. RISCO E INCIDENTES DE SEGURANÇA: CALIBRANDO DIREITOS E DEVERES
3. AGENDA REGULATÓRIA ANPD



29.04.2021 – PALESTRAS

**II Seminário
Internacional – Lei
Geral de Proteção de
Dados: Arquitetura da
privacidade no Brasil**

compartilhe    

<https://dataprivacy.com.br/ii-seminario-internacional-lei-geral-de-protecao-de-dados-arquitetura-da-privacidade-no-brasil/>



1. RISCO E PROTEÇÃO DE DADOS



REGULAÇÃO DE RISCOS COMO PARTE DO SISTEMA NORMATIVO DA PROTEÇÃO DE DADOS:



HISTÓRICO

1ª GERAÇÃO (dec. 60-70)

Estado de bem-estar social
Riscos e deveres do Estado

2ª GERAÇÃO (DEC.70)

Descentralização dos riscos e respostas individuais (consentimento)

3ª GERAÇÃO (DEC. 80)

Descentralização dos riscos e respostas institucionais (DPAs)

4ª GERAÇÃO (DEC. 90)

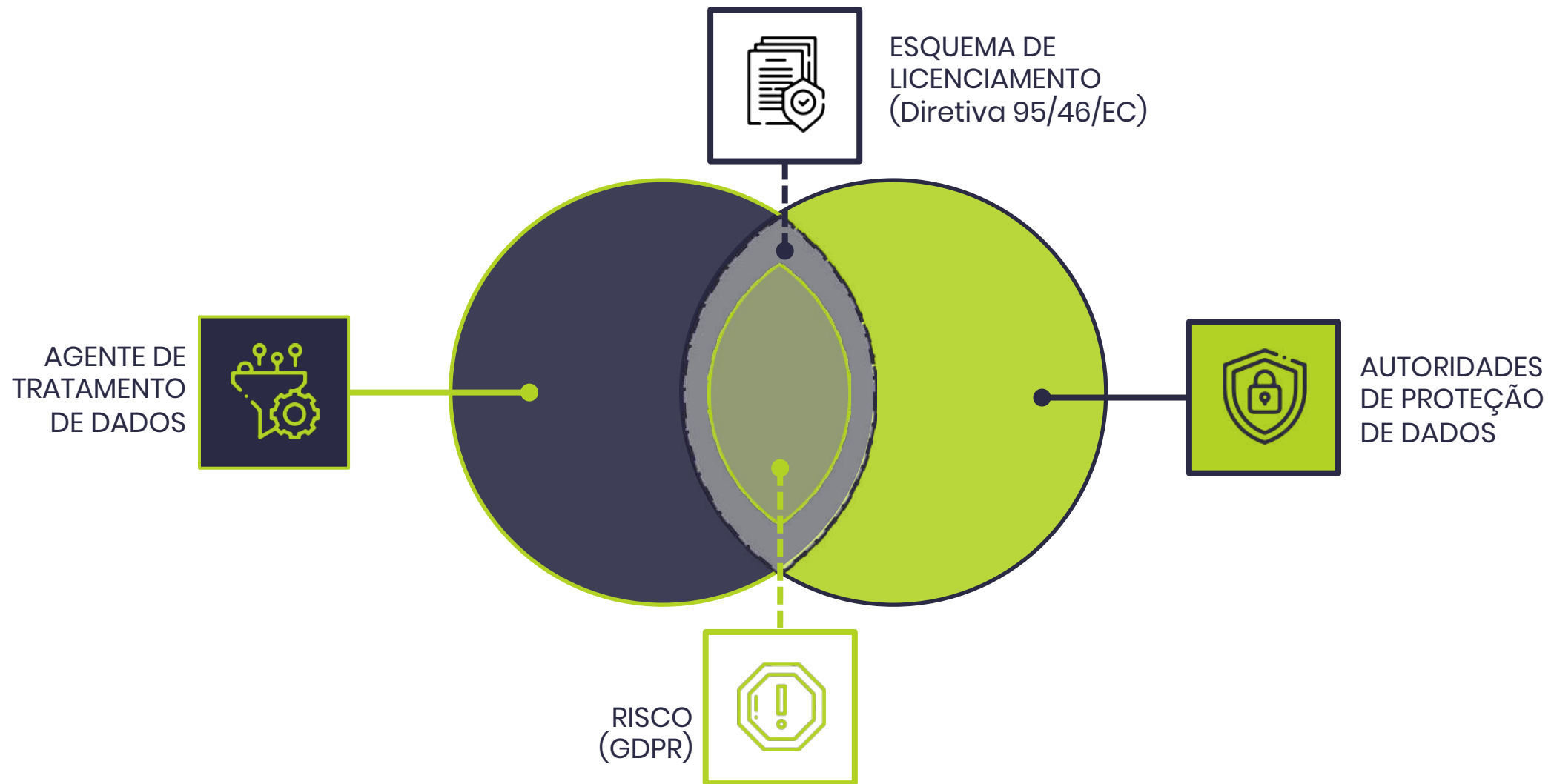
Risco como elemento normativo central (responsabilidade compartilhada)

INTENSIFICAÇÃO (GDPR e LGPD)

- Riscos da perspectiva coletiva
- Participação multissetorial em estratégias de prevenção;
- Metodologias de gestão de riscos.
- Controladores como agentes do manejo de riscos;



NOVAS ABORDAGENS REGULATÓRIAS:





2. RISCO E INCIDENTES DE SEGURANÇA: CALIBRANDO DIREITOS E DEVERES

GARGALOS DE COMPLIANCE

EM RELAÇÃO AO **GDPR** AS SANÇÕES REFERENTES À FALTA DE CUMPRIMENTO DE DEVERES INFORMACIONAIS (AMPLOS E RELATIVOS A INCIDENTES) E A INSUFICIÊNCIA DE MEDIDAS DE SEGURANÇA REPRESENTAM:



MAIS DE 25% DO TOTAL DE MULTAS APLICADAS

DESCUMPRIMENTO DO DEVER DE NOTIFICAÇÃO



17 MULTAS APLICADAS

Valor total de €1,238,291
(aprox. R\$ 8,23 milhões)

INSUFICIÊNCIA DE MEDIDAS PARA GARANTIR A SEGURANÇA DAS INFORMAÇÕES



138 MULTAS APLICADAS

Valor total de €65,904,419 euros
(aprox. R\$ 438,261 milhões)

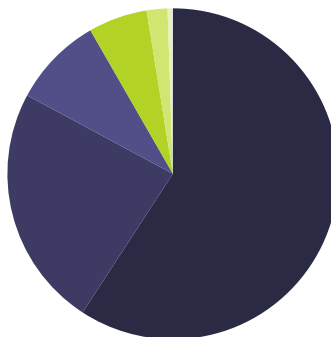
INSUFICIÊNCIA DO CUMPRIMENTOS DE DEVERES DE INFORMAÇÃO



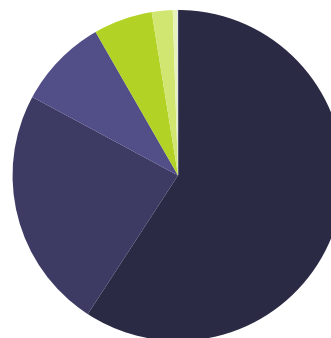
35 Multas aplicadas

Valor total de €5,660,445 euros
(aprox. R\$ 37 milhões)

1. BY TOTAL SUM OF FINES



2. BY TOTAL NUMBER OF FINES

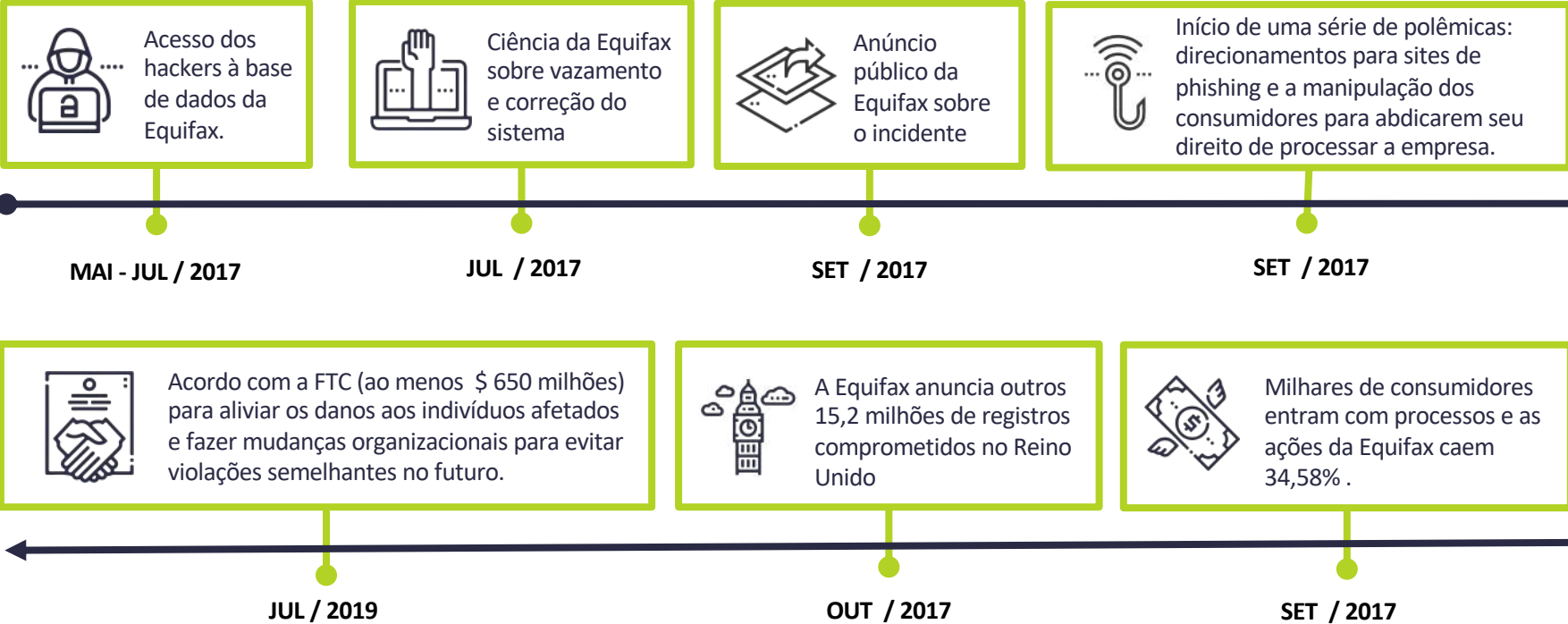


VOLATION	SUM OF FINES
Insufficient legal basis for data processing	€ 164,764,848 (at 229 fines)
Insufficient technical and organisational measures to ensure information security	€ 65,904,419 (at 138 fines)
Non-compliance with general data processing principles	€ 24,618,764 (at 113 fines)
Insufficient fulfilment of data subjects rights	€ 16,024,025 (at 59 fines)
Insufficient fulfilment of information obligations	€ 5,660,445 (at 35 fines)
Insufficient fulfilment of data breach notification obligations	€ 1,238,291 (at 17 fines)
Lack of appointment of data protection officer	€ 186,000 (at 5 fines)
Insufficient cooperation with supervisory authority	€ 183,229 (at 25 fines)
Insufficient cooperation with	€ 89,380 (at 3 fines)
Unknown	€ 500 (at 1 fines)

VOLATION	NUMBER OF FINES
Insufficient legal basis for data processing	229 (with total € 164,764,848)
Insufficient technical and organisational measures to ensure information security	138 (with total € 65,904,419)
Non-compliance with general data processing principles	113 (with total € 24,618,764)
Insufficient fulfilment of data subjects rights	59 (with total € 16,024,025)
Insufficient fulfilment of information obligations	35 (with total € 5,660,445)
Insufficient cooperation with supervisory authority	25 (with total € 183,229)
Insufficient fulfilment of data breach notification obligations	5 (with total € 1,238,291)
Lack of appointment of data protection officer	17 (with total € 1,238,291)
Insufficient data processint agreement	3 (with total € 89,380)
Unknown	1 (with total € 500)

CASO EQUIFAX: LINHA DO TEMPO

CASO EQUIFAX: LINHA DO TEMPO

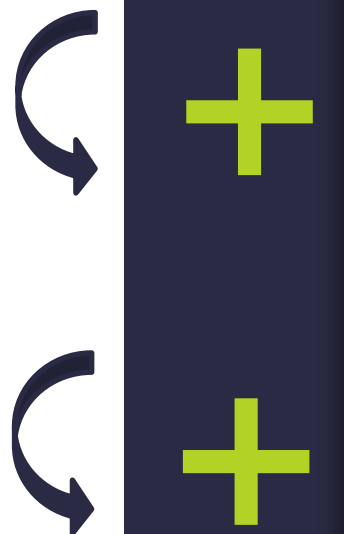


RESULTADOS DO ACORDO



- 1,4 bilhões gastos com a reestruturação informática
- Criação de site para verificação de afetados e registro de usuário no acordo
- Indenização por fraudes e despesas relacionadas
- Ajuda para recuperação e restauração de documentos
- Oferecimento de relatórios de crédito gratuitos

LINHAS DE AÇÃO EM INCIDENTES DE SEGURANÇA



SEM RISCO RELEVANTE

- ✓ Investigação do incidente
- ✓ Documentação do ocorrido
- ✓ Interrupção do ataque, medidas imediatas de contenção
- ✓ Avaliação de riscos e danos



COM RISCO RELEVANTE

- ✓ Notificação dos titulares: Individualmente e/ou geral
- ✓ Notificação da Autoridade Nacional
- ✓ Medidas de mitigação: alterações de padrões de segurança do sistema, avisos para que o titular se proteja, divulgação de canal para titulares sanarem suas dúvidas
- ✓ Produção de relatório sobre o incidente com provisões tomadas e impactos



COM DANO RELEVANTE

- ✓ Divulgação de informações aos titulares sobre reparação de danos
- ✓ Ressarcimento de perdas e danos
- ✓ Controle mais robusto sobre segurança e prevenção de novos incidentes



RISCO EM INCIDENTES DE SEGURANÇA



SEM RISCO RELEVANTE O incidente de segurança deve ser anotado nos registros das atividades de tratamento de dados, especialmente o juízo de valor do porquê foi considerado irrelevante **(REGISTRO)**



COM RISCO RELEVANTE Deve-se não só anotá-lo nos registros das atividades de tratamento de dados, mas, também, notificar os órgãos reguladores e titular e ser ativado um plano de resposta à incidente de segurança **(COMUNICAÇÃO E GESTÃO)**



COM DANO RELEVANTE Deve-se não só anotá-lo nos registros das atividades de tratamento de dados, mas também notificar os órgãos reguladores e o titular e o plano de resposta deve ser mais robusto frente ao do item anterior **(COMUNICAÇÃO, GESTÃO E REPARAÇÃO)**

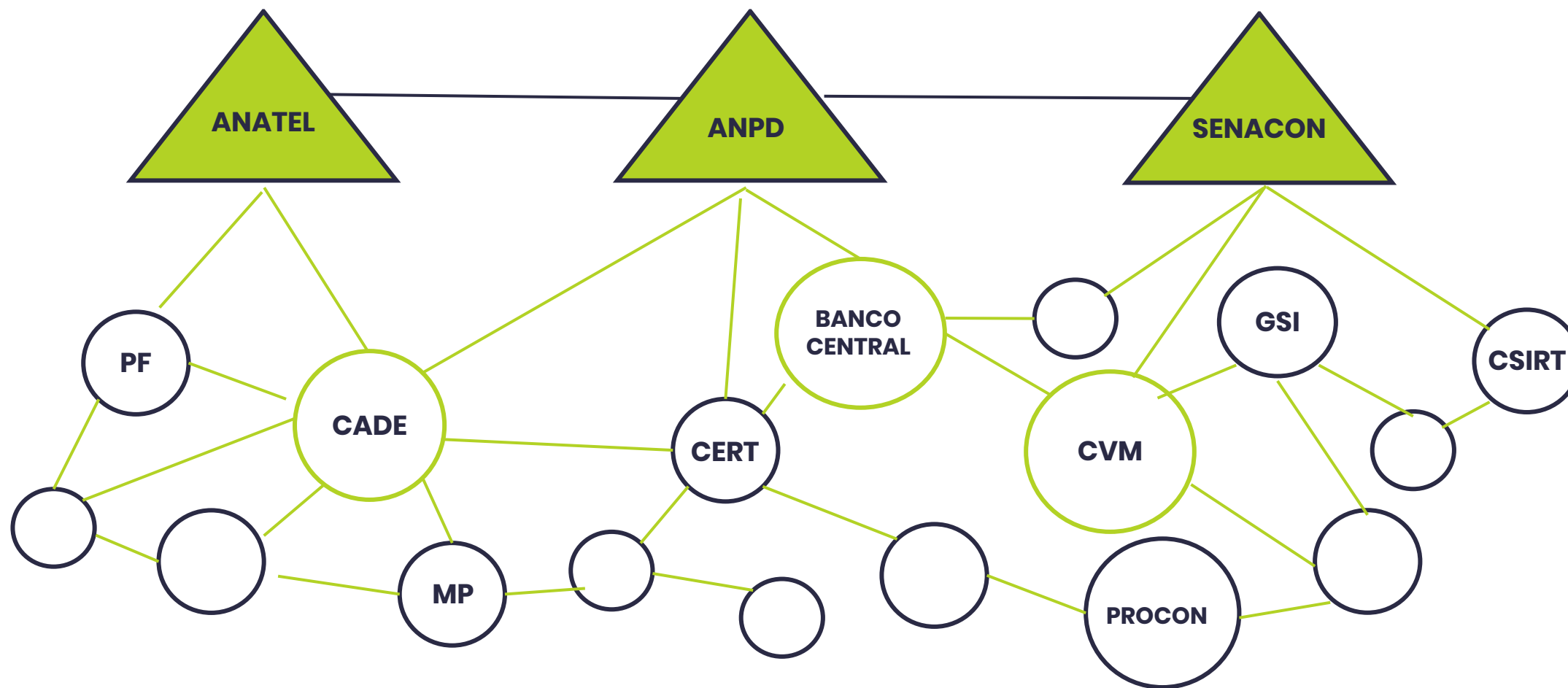


“
Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
”



3. AGENDA REGULATÓRIA ANPD

QUEM SÃO OS NODOS DA REDE E AS FERRAMENTAS PARA ESCALAR ESSA REDE DE GOVERNANÇA?





FDD EM PROJETOS EM PROTEÇÃO DE DADOS

COLETIVIZAÇÃO DA TUTELA

“Uma das principais características da risquificação é justamente a habilitação para que entidades civis tenham legitimidade ativa em processos judiciais contra empresas que tenham violado as normas de proteção de dados pessoais “

ZANATTA, Rafael. 2017

FUNDOS DE FINANCIAMENTO

O sistema de financiamento direto, por outro lado, poderia ser uma expansão de prática já comum nos Estados Unidos de dirigir prêmios cibernéticos em ações coletivas ações judiciais para ONGs de privacidade (...) a lei poderia incentivar que os prêmios sejam canalizados para o fundo público, o que em seguida, certifique-se de que os recursos sejam distribuídos de forma mais ampla e justa.

LANCIERI, Filippo. 2021



DANO REPUTACIONAL



CUSTOS DE UM INCIDENTE DE SEGURANÇA

- Interrupção de negócios e perdas de receita e de tempo de inatividade do sistema;
- Custo de clientes perdidos e aquisição de novos clientes;
- **Perdas de reputação (40% dos gastos).**

PERDAS EM REPUTAÇÃO PELA FALTA DE PRIVACIDADE E SEGURANÇA

PREJUÍZO REPUTACIONAL REPRESENTA CERCA DE 40% DOS GASTOS DE UM INCIDENTE DE SEGURANÇA.

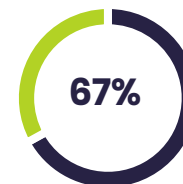


GANHOS EM REPUTAÇÃO COM PRIVACIDADE E SEGURANÇA

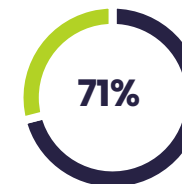
INVESTIMENTOS EM PRIVACIDADE, POR OUTRO LADO, MOSTRAM RETORNOS FINANCEIROS, INCLUSIVE, EM RAZÃO DA MELHORA EM TERMOS REPUTACIONAIS

IMPACTO COMERCIAL DA PRIVACIDADE

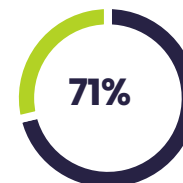
Percentual de empresas com benefícios significativos em cada área, N = 2549



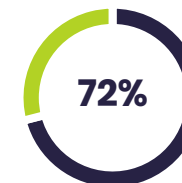
REDUÇÃO DOS ATRASOS DE VENDAS



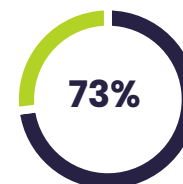
MENOS PERDAS OCASIONADAS POR VIOLAÇÃO DE DADOS



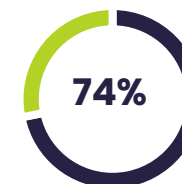
GANHO DE AGILIDADE E INOVAÇÃO



OBTENÇÃO DA EFICIÊNCIA OPERACIONAL DEVIDO AOS CONTROLES DE DADOS



A EMPRESA FICA MAIS ATRAENTE PARA OS INVESTIDORES



DESENVOLVIMENTO DE LEALDADE E CONFIANÇA COM OS CLIENTES



OBRIGADO!

DataPrivacyBR
RESEARCH



ASSOCIAÇÃO
**DATA PRIVACY BRASIL
DE PESQUISA**



[DATAPRIVACY.COM.BR](https://dataprivacy.com.br)



[DATAPRIVACYBRASIL](https://www.instagram.com/dataprivacybrasil)