LGPD COMO SISTEMA DE GESTÃO

Acreditação
LGPD
Fundação Vanzolini

DEMANDA POR PRIVACIDADE DE DADOS

Demanda por privacidade de dados

- **Economia digital:** modelo econômico baseado em serviços fornecidos pela infraestrutura de Tecnologia da Informação e Comunicação: Computação em Nuvem, Inteligência Artificial, Redes de Dispositivos Móveis (5G) e Internet das Coisas (IoT).
- **Privacidade de dados:** demanda recente da sociedade, sobre a qual se apoiam outros direitos, como liberdade de expressão e opinião, inviolabilidade da intimidade e o exercício da cidadania.
- **Autodeterminação informativa:** estabelece que a decisão final é sempre do Titular quanto ao que pode ser feito com seus dados pessoais.
- **Arcabouço legal no Brasil:** Constituição Federal, Lei Geral de Proteção de Dados, Marco Civil da Internet, Código de defesa do Consumidor.
- **Privacidade no mundo:** GDPR (União Europeia), CCPA (Califórnia), SHIELD (Nova York), AEPD (Espanha), ADPA (Áustria), BCDPFI (Berlin).

GDPR - Lei Europeia de Privacidade de Dados

- **GDPR:** European Union General Data Protection Regulation
- **Princípio orientador:** dados pessoais não são das empresas ou do estado.
- **Entrada em vigor:** 25/maio/2018
- **Classificação criticidade de não-conformidades:**
  > Baixa: p.ex. consentimento para menores, obrigações gerais de controladores e operadores.
  > Alta: p.ex. princípios de tratamento de dados, tratamento ilegal, transferência de dados.
- **Multas:**

  (1) até € 10 milhões ou 2% do faturamento, o que for maior.

  (2) até € 20 milhões ou 4% do faturamento, o que for maior.
- **Multas 1º Trimestre de 2020:** Total € 50 milhões.
- **Multas até hoje:** Total € 144 milhões.
- **Maior multa:** Google, € 50 milhões, janeiro de 2019.

Multas de grande impacto

- **British Airways - € 204,6 milhões -** Mecanismos inadequados de segurança da informação, facilitando o roubo de 500 mil registros de clientes.

- **Marriott International - € 110,3 milhões -** Falta de diligência após a aquisição do Grupo Starwood para implementação de medidas de segurança apropriadas, o que levou à exposição de 339 milhões de registros de clientes.

- **Google - € 50 milhões -** Falta de transparência sobre como os dados dos Titulares foram coletados e usados para a segmentação de anúncios.

- **TIM - € 27,8 milhões -** Estratégia de marketing agressiva, contactando não-clientes sem consentimento ou base legal, alguns mais de 150 vezes por mês.

- **Austrian Post - € 18,0 milhões -** Coleta de dados pessoais sem base legal e venda de dados para terceiros, como preferências pessoais, interesses políticos, endereços e outras informações, afetando 3 milhões de pessoas (⅓ da população da Áustria).

- **Facebook - R$ 6,6 milhões -** Venda de informações de 443 mil brasileiros para consultoria de marketing político Cambridge Analytica.

LEI GERAL DE PROTEÇÃO DE DADOS - BRASIL

LGPD (Lei 13.709/2018) – Conceitos principais

- **Objetivo**: proteger dados pessoais de pessoas naturais, ou seja, pessoas físicas.
- **Escopo:** qualquer empresa, organização, instituição pública ou privada que coleta ou que utiliza dados de pessoas físicas precisa se adaptar a ela.
- **Dado pessoal:** "informação relacionada à pessoa natural identificada ou identificável".
- **Dado pessoal sensível:** "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".
- **Papéis:** Titular, Controlador, Operador, Encarregado de Dados, Autoridade Nacional de Proteção de Dados (ANPD), Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDPP).
- **Direitos do Titular:** acesso e correção de dados incompletos, bloqueio ou eliminação de dados, portabilidade de dados, informação sobre tratamento e compartilhamento.
- **Obrigações:** Controlador e Operador devem ter uma gestão rigorosa de tudo o que for feito com os dados dos Titulares.

LGPD – Bases de tratamento

- **I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;**
- **II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:**

  a) cumprimento de obrigação legal ou regulatória pelo controlador;

  b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

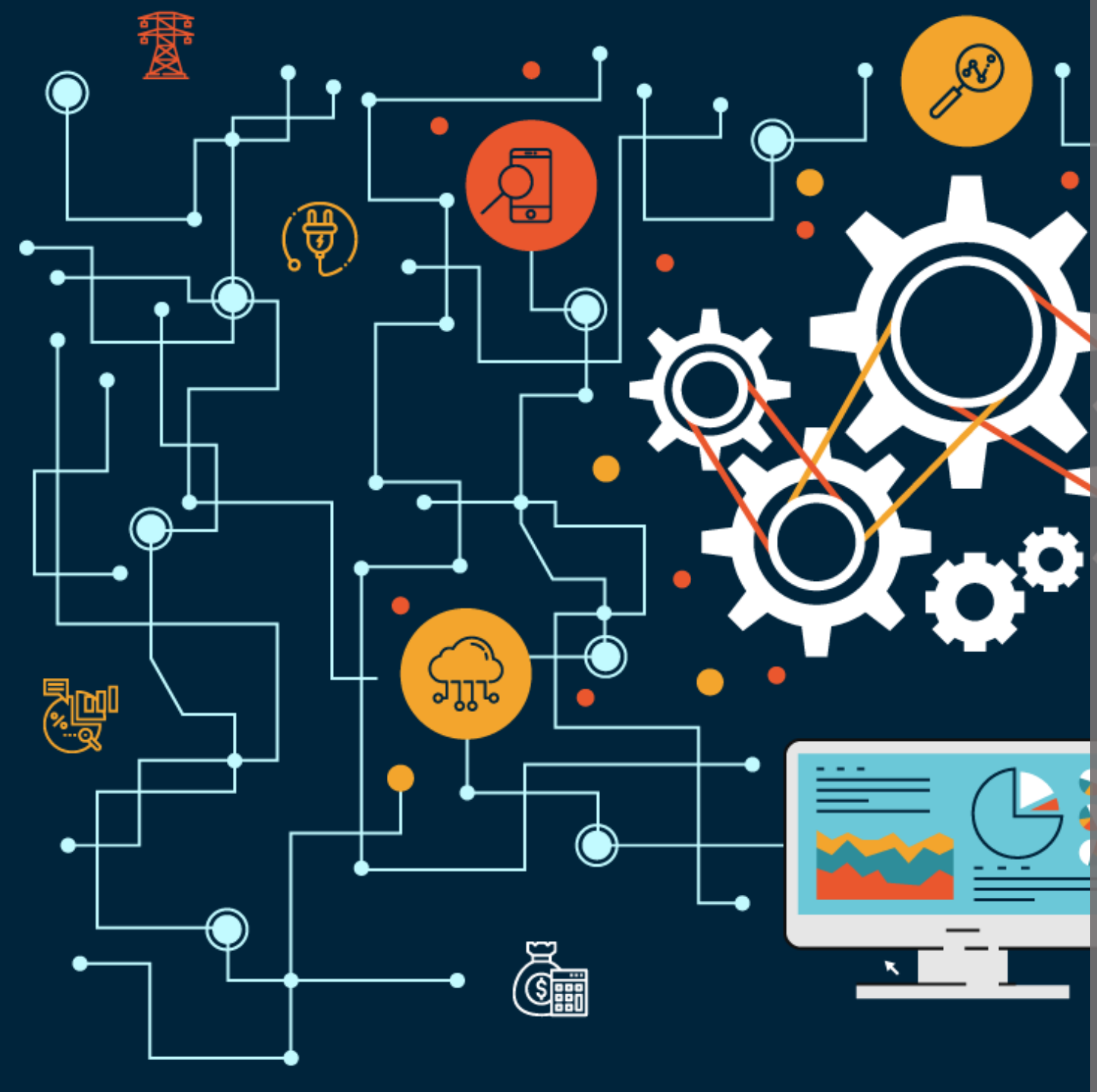
  c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

  d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

  e) proteção da vida ou da incolumidade física do titular ou de terceiro;

  f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

  g) garantia da prevenção à fraude e à segurança do titular.



SISTEMA DE GESTÃO DA PRIVACIDADE DA INFORMAÇÃO

Sistemas de Gestão da Privacidade da Informação

- **Objetivo:** conformidade continuada, previsível e sustentável com os requisitos da LGPD.
- **Público-alvo:** Alta Diretoria, colaboradores, fornecedores, terceiros.
- **Sistema de Gestão:** conjunto de profissionais capacitados, princípios, normas, requisitos, políticas, processos, procedimentos, sistemas de TIC, bases de dados, controles, registros e documentos (p.ex. contratos, relatórios-padrão), todos integrados estrutural e operacionalmente de maneira a garantir a geração continuada, previsível e sustentável de valores de negócio.
- **SGPI:** sistema de gestão da segurança da informação que considera a proteção da privacidade como potencialmente afetada pelo tratamento de dados pessoais.
- **Escopo:** contexto da organização, liderança, planejamento, apoio, operação, avaliação do desempenho, melhoria contínua.
- **Destaques:** liderança da Alta Diretoria, fortalecimento da cultura de privacidade, capacitação de profissionais, gerenciamento de equipes multidisciplinares, controles integrados na infraestrutura de TIC.

Desenvolvimento do SGPI

- **Desafio:** mapeamento de requisitos da LGPD e riscos de não-conformidade em controles do SGPI.
- **Abordagem da FCAV:** foco na transformação organizacional, definindo classes de controles de atendimento de requisitos da LGPD orientados segundo uma visão de negócios na forma de Programas de Transformação da organização, facilitando a implantação, capacitação, operação e melhoria contínua do SGPI.
- **Níveis de atendimento de requisitos:** I-Não atendido; II-Atendido parcialmente; III-Atendido plenamente; IV-Atendimento procedimentalizado; V-Atendimento automatizado.

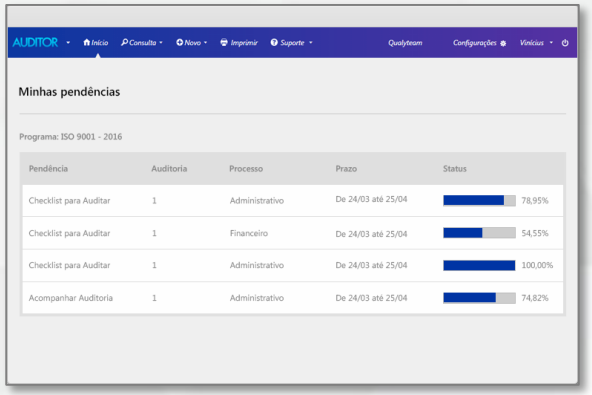
Como evitar multas usando o SGPI?

- **0.1.1 - Estruturação do SG:** Definir o sistema de gestão de cibersegurança e privacidade de dados.
- **6.1.4 - Gestionar requisitos para Informações Protegidas:** Indicar o encarregado pelo tratamento de dados pessoais.
- **6.2.2 - Captura da informação:** Informar tratamentos ao Titular.
- **6.4.3 - Acesso à informação:** Revisar o registro de acesso às informações sensíveis.
- **6.5.5 - Remoção da informação:** Informar ao titular quais dados não serão removidos com base em obrigações legais ou regulatórias específicas do controlador.
- **6.6.1 - Tratamento ético:** Informar ao titular quais dados não serão removidos com base em obrigações legais ou regulatórias específicas do controlador.
- **6.8.2 - Auditoria de segurança e privacidade:** Preparar relatório de impacto à proteção de dados pessoais.
- **8.2.5 - Treinamento:** Realizar treinamentos em manuseio de dados.

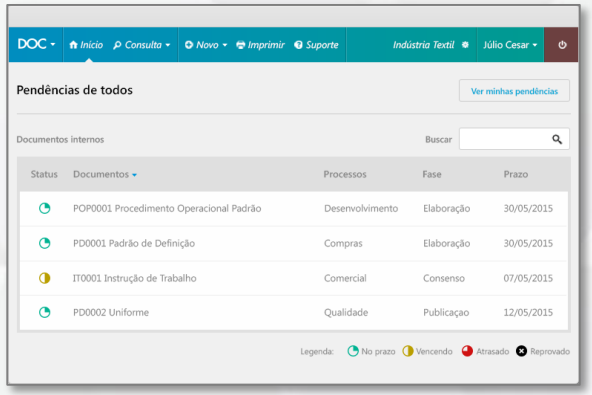
PROJETO DE CONFORMAÇÃO COM A LGPD

Ferramentas de gestão da Qualyteam

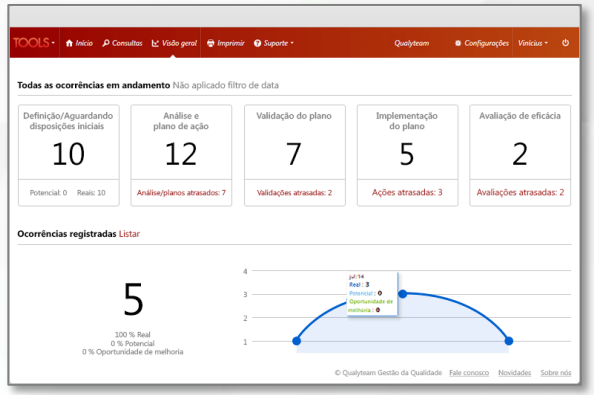
AUDITOR: Gerenciamento de auditorias de conformação com requisitos da LGPD.



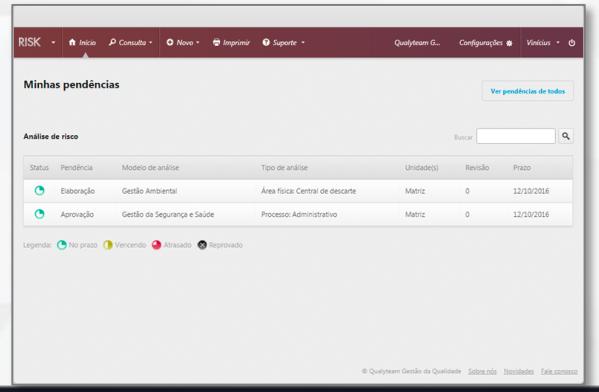
DOC: Gerenciamento de documentos internos, externos e registros da LGPD.



TOOLS: Gerenciamento de não-conformidades com requisitos da LGPD.



RISK: Gerenciamento de riscos de não-conformidades com requisitos da LGPD.



Por que começar HOJE a conformação com LGPD?

- **Oportunidade:** Quando a crise acabar, sua empresa terá fortalecido a cultura de privacidade de dados entre colaboradores e terceirizados.

- **Tempo de transformação:** A liderança da Alta Diretoria pode gerar um movimento de superação do desafio de conformação com a LGPD, unindo diversas áreas da empresa em torno do mesmo objetivo, fortalecendo o espírito de equipe e desafiando os gestores para a inovação de serviços e produtos em conformidade com a Lei.

- **Diferenciação:** Conformidade com a LGPD gera vantagem competitiva e valorização frente aos concorrentes do mercado, assim como acontece com a garantia da qualidade.

- **Redução de riscos:** Risco de sanções da ANPD, bloqueio do uso de dados críticos, riscos de imagem no mercado, todos são obstáculos para ampliação do *market share* e atração de novos negócios.

- **Sinergia:** O esforço de conformação com a LGPD alavanca outras ações de proteção de cibersegurança e governança de digital, blindando a organização contra ataques internos e externos.

FERRAMENTAS DE APOIO

Autoavaliação da conformidade com a LGPD

- **Autoavaliação:** A FCAV preparou um questionário com pontos-chave para você determinar como está o nível de conformidade da sua empresa com a LGPD.

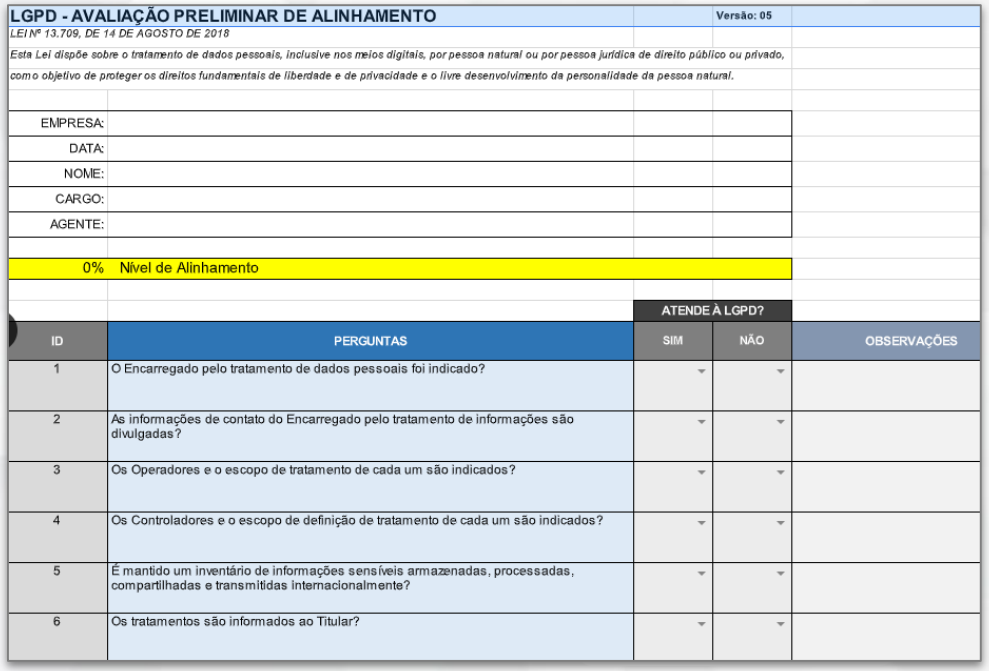
- **Questionário:** São no total 42 perguntas com resposta Sim ou Não, gerando um valor de porcentagem do nível de alinhamento.

- **Exemplos:**

  - *As informações de contato do Encarregado pelo tratamento de informações são divulgadas?*

  - *É garantido o livre acesso facilitado e gratuito ao Titular sobre finalidade, forma e duração do tratamento?*

  - *São realizadas as operações de consolidação, formatação e exportação de dados pessoais para garantia da portabilidade?*



LGPD - AVALIAÇÃO PRELIMINAR DE ALINHAMENTO Versão: 05

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

EMPRESA:	
DATA:	
NOME:	
CARGO:	
AGENTE:	

0% Nível de Alinhamento

		ATENDE À LGPD?		
ID	PERGUNTAS	SIM	NÃO	OBSERVAÇÕES
1	O Encarregado pelo tratamento de dados pessoais foi indicado?			
2	As informações de contato do Encarregado pelo tratamento de informações são divulgadas?			
3	Os Operadores e o escopo de tratamento de cada um são indicados?			
4	Os Controladores e o escopo de definição de tratamento de cada um são indicados?			
5	É mantido um inventário de informações sensíveis armazenadas, processadas, compartilhadas e transmitidas internacionalmente?			
6	Os tratamentos são informados ao Titular?			

Livro: LGPD - Guia de implantação

- **Autores:** Lara Rocha Garcia, Rafael Gonçalves, Marcos Barretto, Edson Aguilera.
- **Editora Blucher - Lançamento: julho/2020**
- **Público-alvo:** Profissionais que buscam uma metodologia para implementar essa transformação cultural de valorização da privacidade de dados pessoais de forma sustentável e perene.
- **Estrutura:**
  - Visão Geral da LGPD;
  - Metodologia BEST de Conformação com a LGPD;
  - Controles para Implantação.

Obrigado !

- **Fundação Carlos Alberto Vanzolini**

  Equipe de Acreditação de Cibersegurança com Foco na LGPD

- **Contato:**
  - Edson Aguilera: edson_aguilera@vanzolini.org.br