

APOIO AO PROCESSO DE GESTÃO DE  
RISCOS E ADEQUAÇÃO AOS REQUISITOS  
DA LEI GERAL DE PROTEÇÃO DE DADOS

# PIRONTI ADVOGADOS



A sociedade Pironi Advogados atua na assessoria e consultoria jurídica altamente especializada nas áreas:

**COMPLIANCE**

**PROTEÇÃO DE DADOS**

**DIREITO DIGITAL  
E INVESTIGAÇÕES  
CORPORATIVAS**

**DIREITO  
ADMINISTRATIVO  
E AMBIENTAL**

**LICITAÇÕES E  
CONTRATOS  
PÚBLICOS**

**CONCESSÕES  
E PARCERIAS**

**PROCESSO  
ADMINISTRATIVO**

**DIREITO DA  
INFRAESTRUTURA  
E REGULAÇÃO**

**GESTÃO DE RISCOS  
NO SETOR PÚBLICO**

**ARBITRAGEM**

**DIREITO  
EMPRESARIAL**

**DIREITO CIVIL**

**DIREITO SOCIETÁRIO**

**FUSÕES E AQUISIÇÕES**

**DIREITO CONTRATUAL**

Dentre outros temas correlatos que demandem profissionais com conhecimento técnico qualificado não só da legislação nacional, como estrangeira.



O Pironi Advogados possui seu escritório principal em Curitiba (Paraná-Brasil), porém, com representação em todo o território Nacional, por meio de alianças específicas, e inserção internacional por meio da renomada **Alianza Jurídica Internacional**, da qual é membro fundador.



# NOSSOS NÚMEROS



**+ 100**

PROFISSIONAIS DIRETOS E INDIRETOS



**+ 130 PROJETOS**

ATUAÇÃO EM  
DE SISTEMA DE INTEGRIDADE E ADEQUAÇÃO À LGPD



**+1.000**

CLIENTES ATENDIDOS



**+50**

ASSESSORIAS EM LICITAÇÕES



**+80**

CLIENTES RECORRENTES

# LEI 13.709/18

A Lei Geral de Proteção de Dados é uma Lei Federal que 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. A Lei entrou em vigor em Setembro de 2020 e a aplicação das sanções iniciaram no dia 1º de agosto de 2021, sendo assim, todas as empresas e instituições públicas que transitam informações de pessoas físicas devem se adequar até essa data.

Ausência de estrutura de segurança para proteção de dados lógicos

Ausência de base legal que garanta a conformidade do tratamento de dados

Ausência de fluxo de tratamento de dados físicos e lógicos

Ausência de um programa de governança em privacidade

Ausência de Política de Segurança da Informação

Ausência de um Plano de Treinamento de Usuários e Operadores de dados



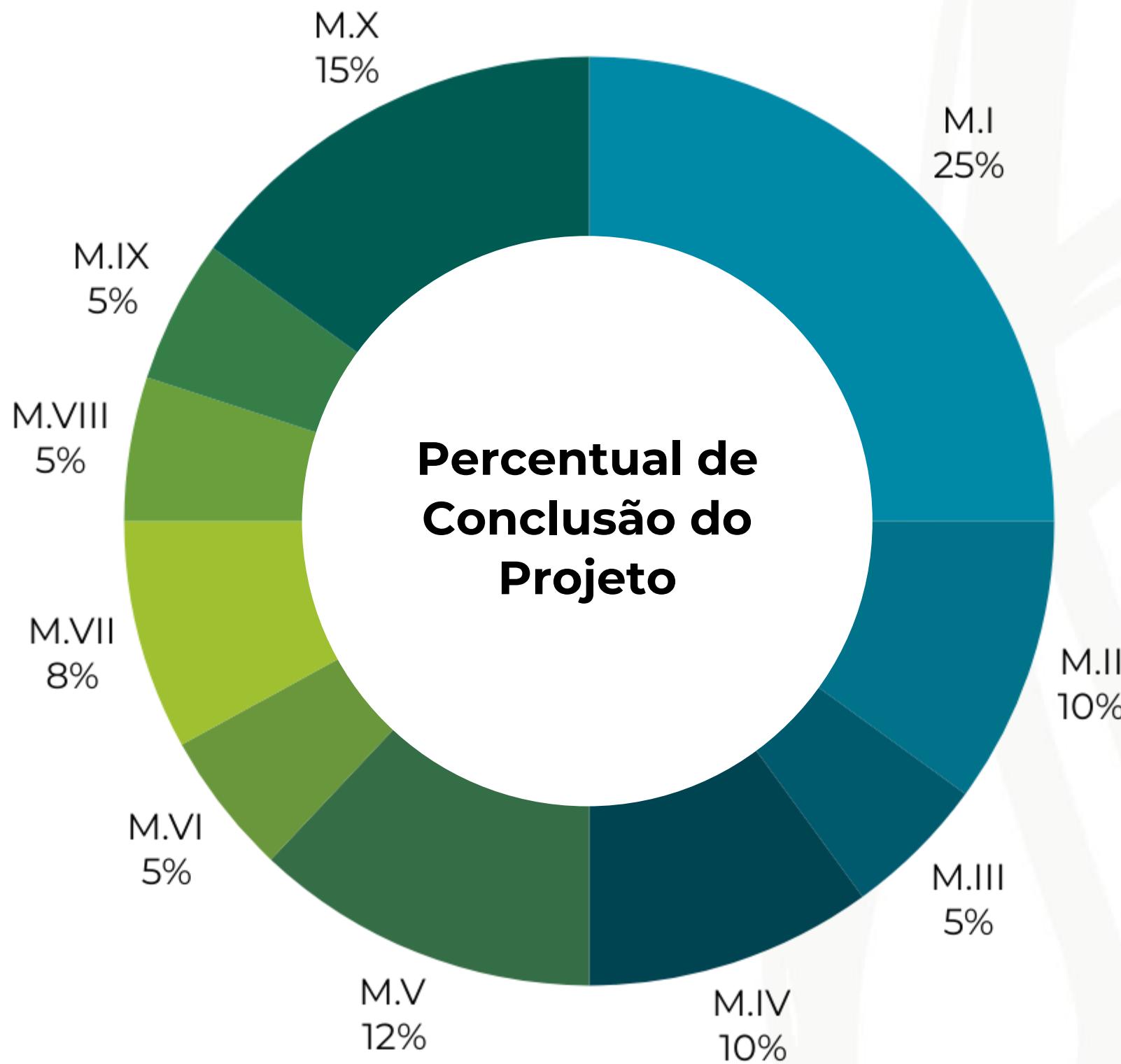
Vazamento de dado não controlado



# MÓDULOS DE APOIO AO PROCESSO DE GESTÃO DE RISCOS E ADEQUAÇÃO



# PERCENTUAL DE CONCLUSÃO DO PROJETO



SISTEMA DE PROTEÇÃO DE DADOS PESSOAIS



Para o processo de apoio à adequação, o escritório Pironti Advogados oferece propostas com valoração modular baseadas em nossa metodologia de trabalho.

# MÓDULO I

## DATA MAPPING & RISK ASSESSMENT

A constante atualização do *Data Mapping & Risk Assessment* é essencial para o processo de adequação à Lei Geral de Proteção de Dados.

Este módulo consolida o mapeamento de todos os tratamentos de dados pessoais que ocorrem na empresa, classifica os riscos decorrentes desses tratamentos e prevê os planos de ação para mitigação e gerenciamentos dos riscos.

Sendo assim, o DM & RA serve como ponto de partida para o processo de implementação do Sistema de Privacidade e adequação à LGPD.



»»»

### ENTREGÁVEIS

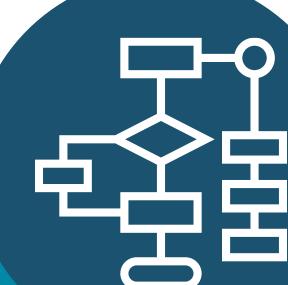
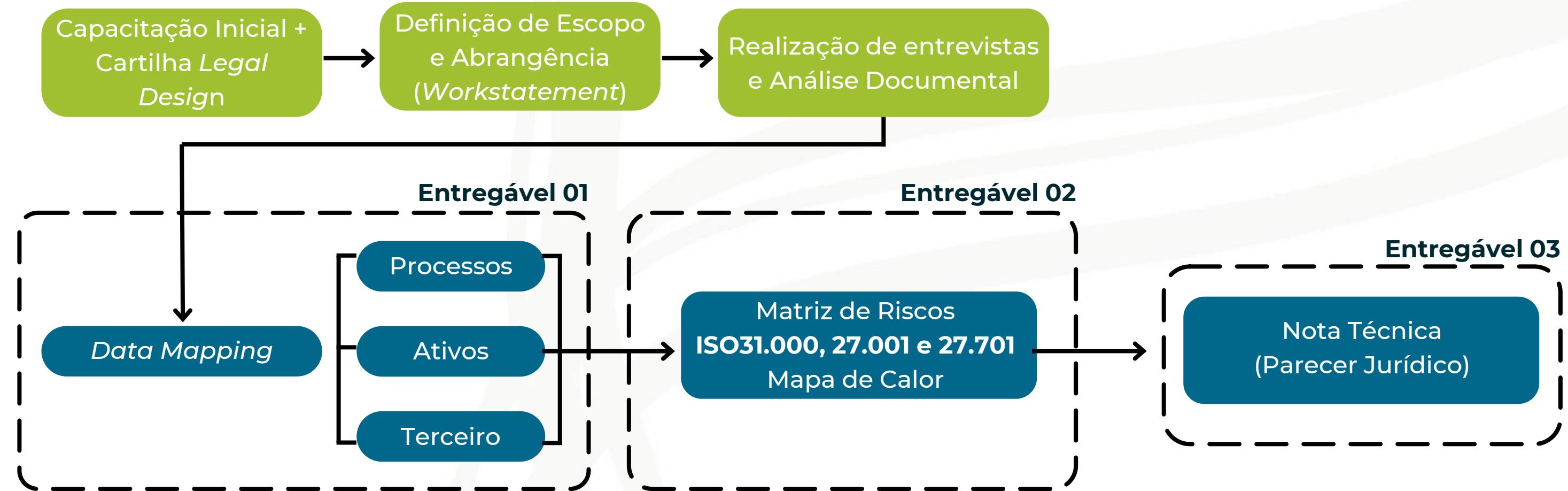
*Data Mapping (Processos | Ativos | Terceiros);*

*Matriz de Riscos ISO 31.000, 27.001 e 27.701;*

*Heat Map (Mapa de Calor) 5x5;*

*Nota Técnica com parecer jurídico acerca da metodologia utilizada para revisão dos entregáveis;*

# FLUXO DE TRABALHO PARA ELABORAÇÃO DO *DATA MAPPING E RISK ASSESSMENT*



# DATA MAPPING + MATRIZ DE RISCOS DE LGPD



# MÓDULO II



# ISO/IEC 27701



## Gestão de Riscos



## HEAT MAP (MAPA DE CALOR 5x5)

PROBABILIDADE

Muito Alta	5	10	15	20	25
					Processos e Ativos: 34
Alta	4	8	12	16	20
		Processos e Ativos: 6	Processos e Ativos: 5	Processos e Ativos: 57	Processos e Ativos: 13
Média	3	6	9	12	15
			4	15	4
Baixa	2	4	6	8	10
		1	4	4	3
Muito baixa	1	2	3	4	5
		3		3	1
Processos e Ativos: 8	Processos e Ativos: 35	Processos e Ativos: 25	Processos e Ativos: 54	Processos e Ativos: 1	
Muito baixa	Muito baixa	Baixa	Média	Alta	Muito Alta

IMPACTO

O resultado da análise de Probabilidade x Impacto culmina na concepção de um **Mapa de Calor 5x5 (Padrão ISO 31.000)**, uma ferramenta de gestão que apoia da celeridade da tomada de decisões acerca do tratamento dos riscos vinculados ao tratamento de dados da Instituição.



## ENTREGÁVEL

Relatórios de Impacto à Proteção de Dados, elaborados conforme análise dos critérios gerais e específicos estabelecidos pela ANPD.

# MÓDULO II

## RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS - RIPD

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) é um documento formal, previsto na LGPD em seu art. 5º inc. XVII e que tem como função principal registrar tratamento de dado pessoal que possua grau de risco elevado para o controlador, bem como ao titular do dado.

Trata-se de uma formalidade inerente ao processo coerente de tratamento de dados pessoais e deve ser elaborado todos os tratamentos de alto risco conforme critérios recentemente estabelecidos pela ANPD.

**AVALIAÇÃO DO RISCO 1 – ID: 5****EVENTO DE RISCO**

Ausência de diretrizes contendo orientações acerca da segurança da informação.

**CAUSAS**

Ausência de Política de Segurança da Informação ou de revisão desta.

**CONSEQUÊNCIAS**

Aplicação de sanções previstas no artigo 52 da LGPD.

**PROBABILIDADE:****RISCO INERENTE:**

16 - Extremo

**IMPACTO:****PLANOS DE AÇÃO PREVENTIVOS**

Política de Segurança da Informação: Elaboração e/ou revisão anual da Política de Segurança da Informação (com senha, controle de vulnerabilidade e possibilidade de criptografia, controle de acessos, WI-FI, backup e troca de informação e processo disciplinar por descumprimento).

**PLANOS DE AÇÃO DE CONTINGÊNCIA**

Plano de Resposta a Incidentes: Criar procedimentos de resposta a incidentes de proteção de dados, contendo protocolos de comunicação à Autoridade Nacional de Proteção de Dados (ANPD), aos titulares e, quando aplicável, aos demais agentes de tratamento de dados pessoais.

**LOGO DO CLIENTE****AVALIAÇÃO DO RISCO 2 – ID: 30****EVENTO DE RISCO**

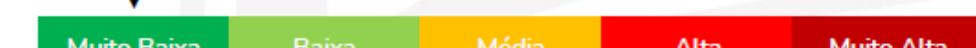
Perda e/ou destruição de dados pessoais e informações confidenciais da Prefeitura.

**CAUSAS**

Ausência de procedimento e de Política de Backup.

**CONSEQUÊNCIAS**

Aplicação de sanções previstas no artigo 52 da LGPD.

**PROBABILIDADE:****RISCO INERENTE:**

5 - Médio

**IMPACTO:**

# MÓDULO III

## ESTRUTURA ORGANIZACIONAL

A Estrutura é formada pelo Encarregado de Dados, também conhecido como *Data Protection Officer (DPO)* e pelo Comitê de Privacidade da empresa.

O DPO possui o importante papel de atuar como um facilitador na comunicação entre empresas, titulares e a Autoridade Nacional de Proteção de Dados (ANPD). Para tanto, exercerá atividades relacionadas ao recebimento das reclamações encaminhadas pelos titulares, prestando os devidos esclarecimentos; receberá as comunicações emitidas pela ANPD, adotando todas as medidas necessárias; bem como deverá emitir orientações para os colaboradores da empresa em relação às boas práticas de proteção de dados pessoais.

Já o Comitê de Privacidade tem o papel de apoiar o DPO nas atividades relacionadas ao gerenciamento dos riscos de proteção de dados, monitoramento das respostas a incidentes, acompanhamento dos planos de ação para mitigação dos riscos e controle de indicadores de desempenho relacionados ao Sistema de Privacidade.



### ENTREGÁVEIS

Nomeação do DPO e do Comitê de Privacidade;

Regimento Interno do Comitê de Privacidade;

Capacitação da Estrutura Organizacional de Proteção de Dados;

Comunicado para divulgação da Estrutura Organizacional de Proteção de Dados.



## ENTREGÁVEIS

- Política de Privacidade;
- Política de Segurança da Informação;
- Política de Cookies;
- Política de *Backup*;
- Política de Senhas;
- Política de Controle de Acessos, dentre outras.

# MÓDULO IV

## POLÍTICAS DE PROTEÇÃO DE DADOS

A revisão, elaboração e implantação de Políticas comportamentais e procedimentais relacionadas ao Sistema de Privacidade de Dados, em conformidade com as devidas priorizações e a necessidade da empresa, são de suma importância para o processo de adaptação à LGPD.

São as políticas que formalizam as novas “regras do jogo” e refletem de maneira clara e objetiva o compromisso da empresa com a privacidade e dispõem sobre a forma de tratamento de dados na execução de sua atividade.

As políticas serão desenvolvidas de acordo com a realidade de cada empresa, conforme diagnosticado nos planos de ação do DM & RA.

# MÓDULO V

## RESPOSTA A INCIDENTE DE SEGURANÇA

O risco é inerente às atividades econômicas e, mesmo que todas as medidas de prevenção e mitigação sejam adotas, ainda assim há a possibilidade de concretização dos riscos mapeados no DM & RA. É essencial, portanto, que a empresa esteja preparada e saiba como atuar caso isso eventualmente aconteça.

Além dos esforços de conservação das informações, a companhia deve se posicionar de forma transparente e assertiva em relação aos titulares e autoridades, de modo a cumprir com o previsto na LGPD.



### ENTREGÁVEIS

Plano de Resposta a Incidentes com fluxo e procedimento;

Protocolo de Comunicação de Incidentes à Autoridade Nacional de Proteção de Dados (ANPD);

Protocolo de Comunicação de Incidentes ao Controlador.



## ENTREGÁVEIS

Revisões em contratos de fornecimento e comerciais que prevejam o tratamento de dados pessoais;

Revisão de cláusulas contratuais referentes ao tratamento de dados pessoais;

Diagnóstico de adequação de terceiros.

# MÓDULO VI

## GESTÃO DE TERCEIROS

É muito comum o envio ou o recebimento de dados e informações entre empresas em decorrência da prestação de serviços ou produtos. Na grande maioria das vezes o tratamento de dados de uma empresa não se limita a esta, havendo uma cadeia de responsabilidade em relação ao tratamento de dados.

Sendo assim, é importante que a empresa conheça o nível de adequação de seus fornecedores e terceiros em relação à LGPD, até pelo fato de que, a depender das atividades realizadas, poderá ser responsabilizada pelas condutas de seus fornecedores e terceiros.

# MÓDULO VII

## DIREITO DOS TITULARES

A LGPD tem como um de seus princípios a autodeterminação informativa, a qual garante ao titular de dados o controle de como os seus dados serão utilizados e para quais finalidades. Sendo assim estes poderão solicitar a confirmação de tratamento, acesso, alteração, anonimização, portabilidade, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei Geral de Proteção de Dados.



### ENTREGÁVEIS

Elaboração de fluxo de resposta aos titulares;

Capacitação do DPO para recebimento de questionamentos e resposta aos titulares;

Protocolos de Resposta aos Titulares que solicitam o exercício de seus direitos.



### ENTREGÁVEIS

Adequação de formulários que coletam consentimento para o tratamento de dados;

Adequação de termos que coletam consentimento para o tratamento de dados;

Apoio na adoção de ferramentas que permitam a gestão do consentimento referente às bases de dados.

## MÓDULO VIII

### GESTÃO DO CONSENTIMENTO

A base legal do consentimento, que é amplamente utilizada pelas empresas, possui requisitos específicos para a sua validade. Além disso, por ser uma concessão do titular de dados, permite com que este possa escolher retirar o consentimento a qualquer momento. Sendo assim, o tratamento de dados realizados com base no consentimento requer uma gestão contínua e eficiente para garantir que este esteja sendo coletado e mantido devidamente.

# MÓDULO IX

## *PRIVACY BY DESIGN*

O módulo referente ao *Privacy by Design* diz respeito à implementação de processos centrados na privacidade dos titulares dos dados. Este módulo é de suma importância, porque demonstra que a empresa prioriza uma atitude proativa e não reativa no que diz respeito ao tratamento de dados e proteção da privacidade.

Sendo assim, o desenho de processos ou o redesenho, quando necessários, são fundamentais para a efetividade do Sistema de Privacidade de Dados da companhia.



### ENTREGÁVEIS

Elaboração e implementação de processos, com foco na proteção da privacidade;

Análise crítica dos processos existentes, com o objetivo de identificação de oportunidades de melhoria;

Redesenho e implementação de processos, com foco na proteção da privacidade.



## ENTREGÁVEIS

Capacitação Inicial sobre os aspectos gerais da LGPD;

Treinamento a todos os funcionários sobre a implantação do Sistema de Privacidade;

Comunicação interna para ampla divulgação aos colaboradores;

Comunicação externa para ampla divulgação aos terceiros e fornecedores;

Constantes revisões dos módulos anteriores e realização de treinamentos que repassem tais revisões aos colaboradores.

# MÓDULO X

## TREINAMENTO E COMUNICAÇÃO

O propósito final do processo de implantação de um Sistema de Privacidade e de adequação à Lei Geral de Proteção de Dados é o estabelecimento de uma cultura organizacional voltada à proteção e respeito ao tratamento de dados de pessoas naturais.

Esse aculturamento pressupõe a realização periódica de uma série de treinamentos e comunicações com a finalidade de gerenciar o maior risco advindo do tratamento de dados: o usuário.

É somente através do constante treinamento e orientação que todos os demais módulos do Sistema de Privacidade serão verdadeiramente incorporados ao dia a dia da empresa.

# CRONOGRAMA DE ATIVIDADES





APOIO AO PROCESSO DE  
MANUTENÇÃO DO  
SISTEMA DE PROTEÇÃO  
DE DADOS

TERCEIRIZAÇÃO DO  
ENCARREGADO DE DADOS (DPO  
AS A SERVICE)

APOIO AO DPO

ATUAÇÃO POR HORA TÉCNICA



# TERCEIRIZAÇÃO DO ENCARREGADO DE DADOS (DPO AS A SERVICE)

A atuação do **Encarregado pelo tratamento de dados pessoais**, ou também chamado como *Data Protection Officer* (DPO), é crucial durante o processo de adequação à LGPD. Sua proatividade é imprescindível para o fluído desempenho da organização nas diversas demandas que surgem no cotidiano das atividades empresariais, além deste figurar como elo de comunicação entre a empresa e a Autoridade Nacional de Proteção de Dados e os titulares de dados pessoais.

Por ser **responsável por gerenciar o Sistema de Privacidade e Proteção de Dados Pessoais na organização**, é essencial que o DPO defina e acompanhe o cumprimento de estratégias para gerir os dados da empresa, incluindo a definição de políticas, diretrizes, papéis, responsabilidades e processos relacionados à gestão de dados. Deve, ainda, identificar problemas, buscar oportunidades, propor iniciativas e monitorar as ações vinculadas ao tratamento de dados, com o objetivo de auxiliar a empresa a alcançar maturidade e segurança no tratamento dos dados colhidos.

Sendo assim, **imprescindível que não haja conflito de interesse** entre os papéis já desempenhados e as novas funções diretamente relacionadas ao papel de DPO. Nesse sentido, surge como melhor prática a modalidade de *DPO as a service*, ou seja, quando o papel é exercido por uma pessoa jurídica externa especializada, a qual tem autonomia e ausência de conflito de interesses para que seja preservada uma atuação isenta na tomada de decisões envolvendo tratamento de dados pessoais.

Portanto, as razões de escolha do *DPO as a service* são várias, porém a mais valiosa é seu **nível de entendimento especializado sobre a LGPD**, e, nesse aspecto, o escritório Pironti Advogados conta com equipe habilitada e preparada para desempenhar o papel em questão, garantindo maior segurança ao cliente.



# TERCEIRIZAÇÃO DO ENCARREGADO DE DADOS (DPO AS A SERVICE)

Contamos com um corpo de profissionais altamente capacitados para oferecimento deste serviço que contempla um pacote completo de suporte à companhia com a realização das seguintes atividades:

- a)Comunicação** com a Autoridade Nacional de Proteção de Dados;
- b)Reporte** de Incidentes de Segurança;
- c)Respostas** a questionamentos advindos de Titulares, Clientes e Parceiros.
- d)Reporte** acerca dos procedimentos adotados pela empresa quanto à LGPD perante seus fornecedores e clientes.
- e)Manutenção** da Matriz de Riscos;
- f)Participação** de Sócio do escritório como membro do Comitê de Implantação/Gestão;
- g)Realização de Treinamentos** periódicos (pacote de 03 horas mensais);
- h)Apoio** ao processo de comunicação interna e externa do Programa de Privacidade; e
- i)Suporte** para elaboração, validação ou recomendações em contratos; novos produtos e ofertas; campanhas de marketing; campanha internas para colaboradores; dentre outras que comportem tratamento de dados.

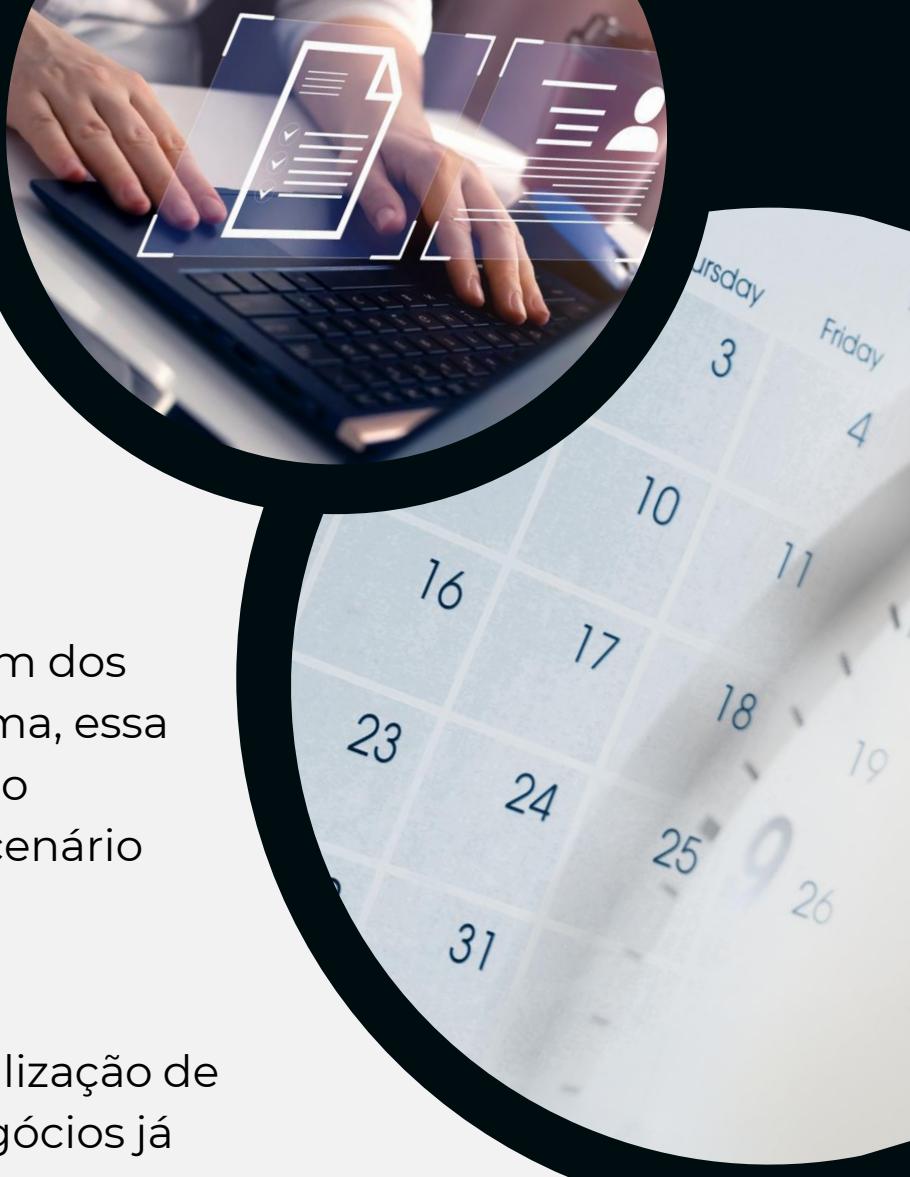


# ATUAÇÃO POR HORA TÉCNICA

**Revisões Contratuais em conformidade com a LGPD (Valor hora):** A gestão eficaz da relação com os terceiros é um dos pontos fundamentais de uma gestão de riscos coerente aos requisitos da Lei Geral de Proteção de Dados, desta forma, essa coerência deve ser refletida nas cláusulas contratuais firmadas com parceiros, clientes e fornecedores. Nossa atuação compreende o entendimento do cenário contratual do cliente, a elaboração de cláusulas contratuais aderentes ao cenário e à legislação e também a participação de nosso time em reuniões para debate técnico com as partes envolvidas.

**Suporte Jurídico Consultivo com a emissão de Pareceres e Opiniões Legais (Valor hora):** Nos dias de hoje a viabilização de novos negócios, nova relações comerciais e inclusive a inserção de novos processos de tratamento de dados em negócios já existentes é permeada por dúvidas acerca da Lei Geral de Proteção de Dados. Nosso corpo técnico busca permanentemente a atualização e capacitação prática para oferecer aos clientes, de forma técnica, soluções adequadas à legislação e à realidade de seu negócio.

**Supporte Consultivo para Revisão/Elaboração de Políticas, Termos e Procedimentos (Valor hora):** A manutenção e o aperfeiçoamento técnico do Sistema de Proteção de Dados Pessoais demanda a revisão permanente de seus documentos para análise crítica e Revisão/Elaboração deste arcabouço com a finalidade de trazer constantemente a garantia da aplicação de melhores práticas de mercado.





 Pirontiadvogados\_ |  pirontiadvogados |  Pironti Advogados  
+55 41 3209-7200 | [www.pirontiadvogados.com](http://www.pirontiadvogados.com)

Av. Vicente Machado, 1001 - 3º andar, Batel | Curitiba/PR