**Diagnóstico e índice de adequação à LGPD**

Prezado respondente, com base nos materiais orientativos publicados pelo Ministério da Economia, adaptamos o seguinte questionário, a fim de oferecer as informações necessárias para um diagnóstico de adequação à Lei Geral de Proteção de Dados – LGPD em seu Órgão/Entidade. O questionário traz também subsídios para a formalização e cálculo de um índice:

|  |  |
| --- | --- |
| Índice | Nível de Adequação |
| 0,00 a 0,29 | Inicial |
| 0,30 a 0,49 | Básico |
| 0,50 a 0,69 | Intermediário |
| 0,70 a 0,89 | Em Aprimoramento |
| 0,90 a 1,00 | Aprimorado |

Esta ferramenta servirá como referência, pois contempla as ações mais relevantes a serem realizadas no caminho da conformidade com a LGPD.

As questões podem ser respondidas com as opções   "Não adota", "Iniciou plano para adotar", "Adota parcialmente" e "Adota Integralmente", conforme descrito:

|  |  |  |
| --- | --- | --- |
| Nível de adoção da prática | Definição | Exemplos |
| Não adota | A organização ainda não adota a prática, bem como não iniciou planejamento para adotá-la. | A organização sabe da necessidade de adotar a prática de elaborar “uma Política de privacidade para cada serviço de forma a informar os direitos dos titulares de dados pessoais, mas não tomou ainda qualquer decisão no sentido de formalizar sua adoção. |
| Iniciou plano para adotar | A organização ainda não adota a prática, mas iniciou ou concluiu planejamento visando adotá-la, o que se evidencia por meio de documentos formais (planos, atas de reunião, estudos preliminares etc.). | Para adotar a prática de elaborar “uma Política de privacidade para cada serviço de forma a informar os direitos dos titulares de dados pessoais, a organização elaborou plano de ação formal que estabelece as atividades, cronograma e responsáveis relativos à elaboração da política. |
| Adota parcialmente | A organização iniciou a adoção da prática, que ainda não está completamente implementada, conforme planejamento realizado; ou a prática não é executada uniformemente em toda a organização. | A prática apresentada é “o órgão já realizou um inventário dos serviços que tratam dados pessoais. A organização, por sua vez, executa o processo de inventários dos dados pessoais apenas para alguns serviços, ou o processo não é executado por todas as suas unidades. |
| Adota integralmente | A organização adota integralmente a prática apresentada, de modo uniforme, o que se evidencia em documentação específica ou por meio do(s) produto(s) ou artefato(s) resultante(s) de sua execução. | Para atender à prática “o órgão já realizou um inventário dos serviços que tratam dados pessoais, a organização possui e executa um processo de inventário dos serviços que tratam dados pessoais utilizados em todas as suas unidades, ainda que o processo não esteja formalmente instituído como norma de cumprimento obrigatório. |

Sugerimos que, após o preenchimento, você salve os resultados (imprimir em PDF).

Grupo de Trabalho sobre LGPD do Governo do Estado de Minas Gerais, instituído pela Resolução Conjunta nº 10.064/2019.

**1 – Governança**

**1 - As partes envolvidas com a implementação da LGPD realizaram a leitura de materiais orientativos, como a** [**Cartilha Lei Geral de Proteção de Dados Pessoais**](https://cge.mg.gov.br/phocadownload/manuais_cartilhas/pdf/Cartilha%20LGPD4%202.pdf) **ou** [**materiais produzidos**](https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd) **pela Secretaria de Governo Digital (Governo Federal)?**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**2 – O art. 50, §2º, I da Lei 13.709/2018 recomenda, como boa prática, a implementação de programa de governança em privacidade.**

**O órgão planejou o seu Programa de Proteção de Dados Pessoais?**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**3 – De acordo com a Lei 13.709/2018, art. 50, inc. I, o controlador poderá formular regras de boas práticas de governança, constando as obrigações específicas para os diversos envolvidos no tratamento de dados, com ações educativas, em programa de governança em privacidade.**

**O órgão desenvolveu um plano de comunicação interno do Programa de Proteção de Dados Pessoais?**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**4 – De acordo com a Lei 13.709/2018, arts. 23 e 41, o Órgão deverá indicar *encarregado*, considerando suas atribuições previstas nesta Lei.**

**O órgão já indicou um encarregado em observância à LGPD?**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**5 - O órgão disponibilizou para o encarregado os recursos necessários para suas atividades e acesso direto à alta administração?**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**6 - O órgão designou os líderes responsáveis por cada frente de atuação no tratamento dos dados? (Lei 13.709/2018, art. 50, caput)**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**7 - Foram definidos indicadores que serão utilizados para medir os resultados do Programa de Proteção de Dados Pessoais? (Lei 13.709/2018, art. 50, *caput*)**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**8 - De acordo com o art. 32, da Lei 13.709/2018, “a autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais”.**

**O órgão elaborou Relatório de Impacto à Privacidade de Dados Pessoais - RIPD?**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**9 - O RIPD foi elaborado com base em orientações de materiais orientativos sobre a LGPD publicados pelo Governo Estadual, ou Federal, como o** [**Guia de Boas Práticas**](https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd) **LGPD (seção 2.5 e Anexo I)?**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**10 - A(s) área(s) envolvidas com tratamento de dados participou(aram) de algum treinamento relacionado com o tema de proteção de dados pessoais?**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**2 - Conformidade legal e respeito aos princípios**

**11 - O órgão, dentro dos limites de suas competências legais, implementou ações para tratar e coletar de forma adequada e não excessiva os dados pessoais dos titulares, em atendimento aos art. 23, 6º, I e III, da Lei 13.709/2018, tratando a mínima quantidade de dados necessários para atingir a finalidade legal desejada?**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**12 - O órgão mapeou os dados pessoais em tratamento e os relacionou à competência legal/finalidade para a qual eles são necessários?**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**13 - O órgão estabeleceu procedimento ou metodologia para verificar se os princípios da LGPD (art. 6º) estão sendo respeitados durante o desenvolvimento de serviços que tratarão dados pessoais desde a fase de concepção do produto ou do serviço até a sua execução (art. 46)?**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**14 - Os princípios da LGPD são aplicados a todo tratamento de dados pessoais realizados pelo órgão, tanto para clientes dos serviços públicos fornecidos quanto servidores, funcionários e/ou colaboradores da instituição?**

 Escolha uma das seguintes respostas:

* Não adota4
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**15 - O órgão conscientizou a(s) área(s) envolvida(s) com tratamento de dados pessoais que a administração pública pode efetuar o tratamento de dados pessoais no exercício de suas competências legais ou execução de políticas públicas para entrega de serviços públicos e que nesses casos não precisará colher o consentimento do titular dos dados?**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**16 - O órgão, ao efetuar o tratamento de dados pessoais no exercício de suas competências legais ou execução de políticas públicas, dá publicidade sobre a finalidade e a forma como os dados serão tratados, de acordo com o inc. VI do art. 6º da LGPD ?**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**17 - O órgão adota sistemas e procedimentos para cumprir o direito de retificação de informações do titular do dado –correção de dados incompletos, inexatos ou desatualizados – de acordo com o art. 18 da LGPD?**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**3 – Transparência, direitos do titular**

**18 - A identidade e as informações de contato do encarregado foram divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador? (Lei 13709/2018, art. 41)**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**19 - O órgão comunica internamente os objetivos do Programa de Proteção de Dados Pessoais?**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**20 - O órgão elaborou uma Política de privacidade para cada serviço de forma a informar os direitos dos titulares de dados e revisou as Políticas de Privacidade já existentes? (Lei 13.709/2018, art. 50, inc. I, alíneas *d* e *h*)**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**21 - As Políticas de Privacidade dos serviços são elaboradas em linguagem simples e acessível? (Lei 13.709/2018, art. 6º, Inc. VI)**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**4 - Rastreabilidade**

**22 - O órgão já realizou um inventário dos serviços/processos que tratam dados pessoais com registros das operações de tratamento? (Lei 13.709/2018, art. 37)**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**23 - O órgão classificou os dados tratados entre dados pessoais e dados pessoais sensíveis? (Lei 13709/2018, arts. 5º, incs. I e II, 46, §1º)**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**24 - O órgão mantém rastreabilidade dos dados do titular seja em formato eletrônico ou físico (papel)? (Lei 13709/2018, art. 46)**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**5 - Adequação de contratos e de relações com parceiros**

**25 - O órgão realizou adequação dos instrumentos convocatórios (como contratos, convênios ou instrumentos congêneres em que haja tratamento de dados pessoais) que estão sendo elaborados? (Lei 13.709/2018, art. 7º, inc. III, 26, §1º e §2º)**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**26 - O órgão já realizou uma revisão dos contratos em vigência para adequá-los à Lei Geral de Proteção de Dados?**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**6 - Segurança da Informação**

**27 - O órgão efetivamente implementou os controles de segurança para os riscos identificados no Relatório de Impacto à Proteção dos Dados Pessoais? (Lei 13709/2018, art. 5º, XVII)**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**28 - O órgão instituiu uma equipe que realiza o monitoramento das vulnerabilidades técnicas dos serviços que tratam dados pessoais?**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**29 - O órgão gera evidências para comprovar que tomou medidas de segurança para proteger os dados pessoais contra ameaças externas e internas?**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**30 - Medidas de segurança são planejadas desde a fase de concepção do produto ou do serviço/processo até a sua execução? (Lei 13.709/2018, art. 46, §2º)**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**7 - Violações de dados**

**31 - O órgão estabeleceu um processo de comunicação das possíveis violações de dados pessoais aos titulares e à Autoridade Nacional de Proteção de Dados (ANPD)? (Lei 13.709/2018, art. 48)**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**32 - O órgão realiza uma gestão de incidentes (plano de resposta e remediação) para tratar possíveis violações dos dados de forma efetiva? (Lei 13.709/2018, art. 50, inc. I, alínea g)**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**33 - O órgão fornece um canal para recebimento de denúncias e de alertas de ocorrências de irregularidades, como denúncias de possíveis vazamento de dados e falhas de segurança e mecanismos de participação do titular? (Lei 13.709/2018, art. 5, Inciso VIII)**

 Escolha uma das seguintes respostas:

* Não adota
* Iniciou plano para adotar
* Adota parcialmente
* Adota integralmente

**Cálculo do Índice de Adequação à LGPD**

|  |  |  |
| --- | --- | --- |
| **Dimensões** | **Índice** | **Nível** |
| **1 - Dimensão Governança** |  |  |
| **2 - Dimensão Conformidade legal e respeito aos princípios** |  |  |
| **3 - Dimensão Transparência e direitos do titular** |  |  |
| **4 - Dimensão Rastreabilidade** |  |  |
| **5 - Dimensão Adequação de contratos e de relações com parceiros** |  |  |
| **6 - Dimensão Segurança da Informação** |  |  |
| **7 - Dimensão Violações de Dados** |  |  |
| **Índice da Adequação à LGPD** |  |  |