

QUESTIONÁRIO – GOVERNANÇA DA DADOS

A – Governança:

- 1. As partes envolvidas com a implementação da LGPD realizaram a leitura do Guia de Boas Práticas sobre a Lei Geral de Proteção de Dados (LGPD) produzido pela Secretaria de Governo Digital?**
 - Sim
 - Não
 - Parcialmente

- 2. O órgão já realizou um planejamento do seu Programa Institucional de Privacidade de Dados?**
 - Sim
 - Não
 - Parcialmente

- 3. O órgão desenvolveu um plano de comunicação interno do Programa Institucional de Privacidade de Dados?**
 - Sim
 - Não
 - Parcialmente

- 4. O órgão já realizou a indicação de um encarregado com conhecimento e experiência suficientes e autonomia para implementar a LGPD?**
 - Sim
 - Não
 - Parcialmente

- 5. O órgão disponibilizou para o encarregado os recursos necessários para implementação da LGPD e acesso direto à alta administração?**
 - Sim
 - Não
 - Parcialmente

- 6. O órgão designou os líderes responsáveis por cada frente de atuação no tratamento dos dados?**
 - Sim
 - Não
 - Parcialmente

- 7. Foram definidos indicadores que serão utilizados para medir os resultados do Programa Institucional de Privacidade de Dados?**
 - Sim
 - Não
 - Parcialmente

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

- Sim
- Não
- Parcialmente

9. O RIPD foi elaborado com base nas orientações da seção 2.5 e Anexo I do Guia de Boas Práticas LGPD?

- Sim
- Não
- Parcialmente

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

- Sim
- Não
- Parcialmente

B- Conformidade legal e respeito aos princípios:

11. O órgão, dentro dos limites de suas competências legais, implementou ações para não tratar e coletar de forma inadequada ou excessiva os dados pessoais dos cidadãos e tratar a mínima quantidade de dados necessários para atingir a finalidade legal desejada?

- Sim
- Não
- Parcialmente

12. O órgão realizou um mapeamento entre os dados processados e a competência legal/finalidade para a qual eles são necessários?

- Sim
- Não
- Parcialmente

13. O órgão estabeleceu procedimento ou metodologia para verificar se os princípios da LGPD 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 (Privacy by Design)?

- Sim
- Não
- Parcialmente

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?

- Sim

- Não
- Parcialmente

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?

- Sim
- Não
- Parcialmente

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 o dado será tratado?

- Sim
- Não
- Parcialmente

17. O órgão adota sistemas e procedimentos para cumprir o direito de retificação de informações do titular do dado?

- Sim
- Não
- Parcialmente

C- Transparência e 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?

- Sim
- Não
- Parcialmente

19. O órgão comunica internamente os objetivos do Programa Institucional de Privacidade de Dados?

- Sim
- Não
- Parcialmente

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?

- Sim
- Não
- Parcialmente

21. As Políticas de Privacidade dos serviços são elaboradas em linguagem simples e acessível?

- Sim
- Não
- Parcialmente

D – Rastreabilidade

22. O órgão já realizou um inventário dos serviços que tratam dados pessoais?

- Sim
- Não
- Parcialmente

23. O órgão já realizou uma classificação dos dados tratados em dados pessoais e dados pessoais sensíveis?

- Sim
- Não
- Parcialmente

24. O órgão mantém rastreabilidade dos dados do titular seja em formato eletrônico ou físico (papel)?

- Sim
- Não
- Parcialmente

E - Adequação de contratos e de relações com parceiros

25. O órgão já realizou uma adequação dos instrumentos convocatórios que estão sendo elaborados?

- Sim
- Não
- Parcialmente

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

- Sim
- Não
- Parcialmente

F – 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?

- Sim
- Não
- Parcialmente

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

- Sim
- Não
- Parcialmente

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

- Sim
- Não
- Parcialmente

30. Medidas de segurança são planejadas desde a fase de concepção do produto ou do serviço até a sua execução (Security by Design)?

- Sim
- Não
- Parcialmente

G- Violação de Dados

31. Sim O órgão estabeleceu um processo de comunicação das possíveis violações de dados pessoais?

-
- Não
- Parcialmente

32. O órgão realiza uma gestão de incidentes para tratar possíveis violações dos dados de forma efetiva?

- Sim
- Não
- Parcialmente

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?

- Sim
- Não
- Parcialmente