A-1 - Governança

A1. 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?

O Guia de Boas Práticas da LGPD pode ser acessado no link: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia_lgpd.pdf

Não adota ☐

Iniciou plano para adotar ☐

Adota parcialmente ☒

Adota integralmente ☐

A2. 2 - O órgão já realizou um planejamento do seu Programa Institucional de Privacidade de Dados?

Lei 13.709/2018, art. 50 Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 2º I : implementar programa de governança em privacidade ...

ABNT NBR ISO/IEC 27701:2019 - 6.3.1.1 Responsabilidades e papéis da segurança da informação.

☐

Não adota ☒

Iniciou plano para adotar ☐

Adota parcialmente ☐

Adota integralmente ☐

A3. 3 - O órgão desenvolveu um plano de comunicação interno do Programa Institucional de Privacidade de Dados?

Lei 13.709/2018, art. 50 Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

I - implementar programa de governança em privacidade... ☐

Não adota ☒

Iniciou plano para adotar ☐

Adota parcialmente ☐

Adota integralmente ☐

A4.

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

Lei 13.709/2018, art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais.

Lei 13.709/2018, art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 2º As atividades do encarregado consistem em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Não adota ☐

Iniciou plano para adotar ☐

Adota parcialmente ☐

Adota integralmente ☒

A5.

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

Lei 13.709/2018, art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 2º As atividades do encarregado consistem em:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Não adota ☐

Iniciou plano para adotar ☐

Adota parcialmente ☐

Adota integralmente ☒

A6.

6 - O órgão designou os líderes responsáveis por cada frente de atuação no tratamento dos dados?

É necessário estipular quais serão os líderes responsáveis por cada frente de atuação como, por exemplo, comunicação com o cidadão, operações de TI, segurança da informação, jurídico, etc.

Lei 13.709/2018, art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Não adota ☐

Iniciou plano para adotar ☐

Adota parcialmente ☐

Adota integralmente ☒

A7.

7 - Foram definidos indicadores que serão utilizados para medir os resultados do Programa Institucional de Privacidade de Dados?

Lei 13.709/2018, art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança...

Não adota [X]

Iniciou plano para adotar [ ]

Adota parcialmente [ ]

Adota integralmente [ ]

A8.

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

Lei 13709/2018, art. 5º, XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

ABNT NBR ISO/IEC 27701-2019 -

5.6.2 Avaliação de riscos de segurança da informação

5.6.3 Tratamento de riscos de segurança da informação

Guia de Boas Práticas da LGPD (seção 2.5) pode ser acessado no link: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia lgpd.pdf

Não adota [ ]

Iniciou plano para adotar [X]

Adota parcialmente [ ]

Adota integralmente [ ]

A9.

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

O Guia de Boas Práticas da LGPD pode ser acessado no link: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia lgpd.pdf

Não adota [ ]

Iniciou plano para adotar [X]

Adota parcialmente [ ]

Adota integralmente [ ]

A10.

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

Lei 13.709/2018, art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas...

Não adota ☐

Iniciou plano para adotar ☐

Adota parcialmente ☐

Adota integralmente ☒

B: 2 - Conformidade legal e respeito aos princípios

B1.

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?

Lei 13709/2018, art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Lei 13.709/2018, art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

Não adota ☐

Iniciou plano para adotar ☒

Adota parcialmente ☐

Adota integralmente ☐

B2.

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

Lei 13709/2018, art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Lei 13.709/2018, art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

Não adota ☐

Iniciou plano para adotar ☐

Adota parcialmente ☐

Adota integralmente ☒

B3.

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)?

Lei 13709/2018, art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Guia de Boas Práticas LGDP, seção 4.1 Privacidade desde a concepção e por padrão (Privacy by Design e by Default).

O Guia pode ser acessado no link: https://www.gov.br/governodigital/pt br/governanca-de-dados/guia-lgpd.pdf

.

Não adota ☐

Iniciou plano para adotar ☒

Adota parcialmente ☐

Adota integralmente ☐

B4.

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?

Lei 13.709/2018, art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial;

Lei 13.709, Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

.

Não adota ☐

Iniciou plano para adotar ☒

Adota parcialmente ☐

Adota integralmente ☐

B5.

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?

Lei 13.709/2018, art. 7º:

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

.

Não adota ☒

Iniciou plano para adotar ☐

Adota parcialmente ☐

Adota integralmente ☐

B6.

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?

Lei 13.709/2018, art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

.

Não adota ☒

Iniciou plano para adotar ☐

Adota parcialmente ☐

Adota integralmente ☐

B7.

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

Lei 13.709/2018, art. 18 O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: III - correção de dados incompletos, inexatos ou desatualizados;

.

Não adota ☒

Iniciou plano para adotar ☐

Adota parcialmente ☐

Adota integralmente ☐

C: 3 - Transparência e direitos do titular

C1.

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 O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

Não adota ☐

Iniciou plano para adotar ☐

Adota parcialmente ☐

Adota integralmente ☒

C2.

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

Lei 13.709/2018, art. 50 Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Não adota ☐

Iniciou plano para adotar ☒

Adota parcialmente ☐

Adota integralmente ☐

C3.

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, CAPÍTULO III DOS DIREITOS DO TITULAR

Lei 13.709/2018, art. 50 Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

I - implementar programa de governança em privacidade que :

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

Não adota ☐

Iniciou plano para adotar ☒

Adota parcialmente ☐

Adota integralmente ☐

C4.

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

Lei 13.709/2018, art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

Não adota ☒

Iniciou plano para adotar ☐

Adota parcialmente ☐

Adota integralmente ☐

D: 4 - Rastreabilidade

D1.

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

Lei 13.709/2018, art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Não adota ☐

Iniciou plano para adotar ☒

Adota parcialmente ☐

Adota integralmente ☐

D2.

23 - O órgão já realizou uma classificação dos dados tratados entre dados pessoais e dados pessoais sensíveis?

Lei 13709/2018, art. 46 Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

Lei 13.709/2018, art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - 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, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Não adota ☐

Iniciou plano para adotar ☒

Adota parcialmente ☐

Adota integralmente ☐

D3.

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

Lei 13709/2018, art. 46 Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito..

- Não adota ☒
- Iniciou plano para adotar ☐
- Adota parcialmente ☐
- Adota integralmente ☐

E: 5 - Adequação de contratos e de relações com parceiros

E1.

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

Lei 13.709/2018, art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

Lei 13.709/2018, art. 26 O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto: IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos.

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

- Não adota ☐
- Iniciou plano para adotar ☒
- Adota parcialmente ☐
- Adota integralmente ☐

E2.

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

Lei 13.709/2018, art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

Lei 13.709, Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto: IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos.

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

- Não adota ☐
- Iniciou plano para adotar ☒
- Adota parcialmente ☐
- Adota integralmente ☐

F: 6 - Segurança da Informação

F1.

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 - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

ABNT NBR ISO/IEC 27701:2019

5.6.2 Avaliação de riscos de segurança da informação

ABNT NBR ISOIEC 27005-2019

8.2.4 Identificação dos controles existentes e planejados

Guia de Boas Práticas da LGPD (seção 2.5) pode ser acessado no link: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia lgpd.pdf

- [ ] Não adota
- [x] Iniciou plano para adotar
- [ ] Adota parcialmente
- [ ] Adota integralmente

F2.

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

Lei 13.709/2018, art. 46 Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

ABNT NBR ISOIEC 27005-2019

8.2.5 Identificação das vulnerabilidades

ABNT NBR ISOIEC 27701-2019

6.9.6 Gestão de vulnerabilidades técnicas

- [x] Não adota
- [ ] Iniciou plano para adotar
- [ ] Adota parcialmente
- [ ] Adota integralmente

F3.

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

Lei 13.709/2018, art. 46 Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Lei 13.709/2018, 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.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

- [x] Não adota
- [ ] Iniciou plano para adotar
- [ ] Adota parcialmente
- [ ] Adota integralmente

F4.

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

Lei 13.709/2018, art. 46 Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Guia de Boas Práticas LGDP, seção 4.1 Privacidade desde a concepção e por padrão (Privacy by Design e by Default). O Guia pode ser acessado no link https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf

- [x] Não adota
- [ ] Iniciou plano para adotar
- [ ] Adota parcialmente
- [ ] Adota integralmente

G: 7 - Violações de dados

G1.

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

Lei 13.709/2018, 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.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

- [x] Não adota
- [ ] Iniciou plano para adotar
- [ ] Adota parcialmente
- [ ] Adota integralmente

G2.

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

Lei 13.709/2018, art. 46 Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Lei 13.709/2018, 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.

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

Lei 13.709/2018, art. 50 Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: I - implementar programa de governança em privacidade que, no mínimo: g) conte com planos de resposta a incidentes e remediação; e

ABNT NBR ISO/IEC 27701-2019

6.13 Gestão de incidentes de segurança da informação

- [ ] Não adota
- [x] Iniciou plano para adotar
- [ ] Adota parcialmente
- [ ] Adota integralmente

G3.

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?

Lei 13.709/2018, art. 5, Inciso VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Lei 13.709/2018, art. 50 Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

§ 2º, Inciso I - implementar programa de governança em privacidade que, no mínimo:

e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

ABNT NBR ISOIEC 27701-2019

6.13.1.2 Notificação de eventos de segurança da informação

- [ ] Não adota
- [ ] Iniciou plano para adotar
- [x] Adota parcialmente
- [ ] Adota integralmente