BABILON
AUDITORIA • CONSULTORIA • LGPD

IMPLEMENTANDO A NR01 COM LGPD

1. DEFINA A BASE LEGAL PARA TRATAMENTO DE DADOS

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

- Defina e documente qual é a base legal prevista na LGPD que justifica o tratamento de dados (ex: **cumprimento de obrigação legal ou regulatória**, no caso da NR-01).
- Dados de saúde são considerados **dados sensíveis** e exigem bases legais específicas (art. 11 da LGPD).

2. FINALIDADE ESPECÍFICA

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;

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados,

I - finalidade específica do tratamento;

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

- Os dados coletados no processo de gerenciamento de riscos ocupacionais devem ser usados **exclusivamente para os fins** previstos na NR-01 (segurança, saúde ocupacional, prevenção de riscos etc.).
- Evite uso secundário (ex: usar para fins comerciais, marketing ou estatísticas sem anonimização).
- Obrigação legal/regulatória**:** Ex. CAT, exames, PGR;
- Execução de contrato**:** Treinamentos, fichas de EPI;
- Exercício regular de direitos: Comunicação com sindicatos, ações trabalhistas.

3. TRANSPARÊNCIA COM O TRABALHADOR

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:

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:

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular

- Os trabalhadores devem ser informados, de forma clara, sobre:
  - ✓ Quais dados estão sendo coletados
  - ✓ Por que estão sendo coletados
  - ✓ Quem terá acesso
  - ✓ Como serão armazenados
- Isso pode ser feito via **política de privacidade** ou **termo de consentimento informado**, se aplicável.
- Tenha **políticas claras** e canais de atendimento para solicitações (“canal do titular”).

4. MINIMIZAÇÃO DE DADOS

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

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;

- Coletar apenas os dados **estritamente necessários** para cumprir a NR-01.
- Exemplo: não coletar dados de saúde que não tenham relação com a atividade ocupacional ou risco identificado.

5. SEGURANÇA DA INFORMAÇÃO

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

VII - segurança: utilização de medidas 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 difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

Art. 13. Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

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.

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.

- Implementar medidas técnicas e administrativas para proteger os dados coletados:

    - ✓ Controle de acesso
    - ✓ Criptografia
    - ✓ Armazenamento seguro (físico e digital)
    - ✓ Backup seguro
    - ✓ Sistemas com autenticação forte

6. CONTROLE DE ACESSO E CONFIDENCIALIDADE

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

VII - segurança: utilização de medidas 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 difusão;

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

II - fim do período de tratamento;

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:

§ 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo

- Acesso às informações sensíveis deve ser restrito a profissionais autorizados, como o médico do trabalho ou equipe de SST.
- Treinar os responsáveis sobre **confidencialidade e sigilo profissional**.

7. RETENÇÃO E DESCARTE ADEQUADO DOS DADOS

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

II - fim do período de tratamento;

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados

- Os dados devem ser mantidos **pelo tempo necessário** para cumprir a legislação trabalhista e de saúde ocupacional.
- Após o prazo, devem ser **eliminados com segurança**, exceto quando exigido por lei manter (ex: histórico de exames periódicos).

8. COMPARTILHAMENTO COM TERCEIROS

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:

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

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

§ 3º A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências.

§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir

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:

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.

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.

- Se houver necessidade de compartilhar dados com terceiros (ex: clínicas, sistemas de SST, consultorias), deve-se:

    - ✓ Verificar contratos com cláusulas de proteção de dados
    - ✓ Garantir que o terceiro esteja também em conformidade com a LGPD
    - ✓ Só podem ser acessados por pessoas autorizadas (ex: médico do trabalho, segurança, jurídico).

9. REGISTRO DAS OPERAÇÕES DE TRATAMENTO

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.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

- Manter um registro interno de todas as atividades de tratamento de dados feitas no âmbito da NR-01, conforme art. 37 da LGPD

10. NOMEAÇÃO DE UM ENCARREGADO (DPO)

Art. 5º Para os fins desta Lei, considera-se:

VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)

Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.

- Ter um responsável (DPO – Data Protection Officer) para atender solicitações dos titulares e da ANPD, especialmente em empresas de médio e grande porte

11. AUDITORIAS E REVISÕES REGULARES

- Avaliar periodicamente se os procedimentos relacionados à NR-01 continuam em conformidade com a LGPD.

12. ATENDIMENTO AOS DIREITOS DOS TITULARES

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:

V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;

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:

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular

- Garantir que o trabalhador possa exercer seus direitos previstos na LGPD:
  - ✓ Acesso aos dados
  - ✓ Correção
  - ✓ Informação sobre compartilhamento
  - ✓ Eliminação, quando aplicável
  - ✓ Revogação do consentimento (quando essa for a base legal)

BABILON
AUDITORIA • CONSULTORIA • LGPD

CHECKLIST DE CONFORMIDADE LGPD - NR-01

Item	Descrição	Situação	Observações
1. Base Legal Identificada	A base legal para tratamento de dados (ex: obrigação legal/regulatória) foi devidamente documentada?	☐ Sim ☐ Não ☐ Parcial	
	Ao aplicar a NR01, foi observado as demais NR? (NR-06, NR-10, NR-35 ...).	☐ Sim ☐ Não ☐ Parcial	
	Foi nomeado o profissional responsável pela elaboração do PGR	☐ Sim ☐ Não ☐ Parcial	
2. Coleta de Dados Necessários	Apenas os dados estritamente necessários para cumprimento da NR-01 são coletados?	☐ Sim ☐ Não ☐ Parcial	
	A necessidade de cada dado coletado é justificada? (sem excesso de dados)	☐ Sim ☐ Não ☐ Parcial	
	O Inventário de Riscos evita identificação direta de trabalhadores?	☐ Sim ☐ Não ☐ Parcial	
	Existe mapeamento dos dados pessoais tratados ?	☐ Sim ☐ Não ☐ Parcial	
3. Dados Sensíveis Identificados	Os dados de saúde ocupacional e outros sensíveis foram corretamente classificados e tratados com proteção especial?	☐ Sim ☐ Não ☐ Parcial	
	Dados sensíveis (exames, CATs) são acessados apenas por pessoas autorizadas?	☐ Sim ☐ Não ☐ Parcial	
	Os dados sensíveis estão protegidos (criptografia, senhas, arquivos seguros)?	☐ Sim ☐ Não ☐ Parcial	
4. Política de Privacidade Disponível	Existe uma política de privacidade clara informando aos trabalhadores sobre uso de seus dados?	☐ Sim ☐ Não ☐ Parcial	
5. Consentimento (se necessário)	Quando o tratamento não se baseia em obrigação legal, foi obtido consentimento válido do trabalhador?	☐ Sim ☐ Não ☐ Parcial	
6. Transparência ao Titular	Os trabalhadores foram informados sobre quais dados são coletados, por quê, por quem e por quanto tempo?	☐ Sim ☐ Não ☐ Parcial	
7. Registro de Operações de Tratamento	Existe registro das atividades de tratamento conforme o art. 37 da LGPD?	☐ Sim ☐ Não ☐ Parcial	
8. Acesso Restrito aos Dados	Os dados pessoais e sensíveis têm acesso restrito e controlado (ex: apenas equipe de SST ou médico)?	☐ Sim ☐ Não ☐ Parcial	
9. Segurança da Informação	Estão implementadas medidas técnicas e administrativas para proteção dos dados (ex: criptografia, backup, controle de acesso)?	☐ Sim ☐ Não ☐ Parcial	

	Há políticas e controles de segurança aplicados ao ambiente de SST?	☐ Sim ☐ Não ☐ Parcial	
	Existe plano de resposta a incidentes de segurança de dados?	☐ Sim ☐ Não ☐ Parcial	
	Backups e logs dos dados pessoais são protegidos adequadamente?	☐ Sim ☐ Não ☐ Parcial	
	Fichas de EPI, listas de presença e outros documentos com nome e assinatura são protegidos contra divulgação indevida?	☐ Sim ☐ Não ☐ Parcial	
	Os registros de treinamentos obrigatórios (NR-01) são armazenados com proteção e acesso controlado?	☐ Sim ☐ Não ☐ Parcial	
	Existe um mapeamento (relatório de impacto - RIPD) dos dados tratados em SST?	☐ Sim ☐ Não ☐ Parcial	
	Há treinamento básico em LGPD para profissionais de RH, SESMT, jurídico ou gestores que lidam com SST?	☐ Sim ☐ Não ☐ Parcial	
	Há integração entre o PGR e as exigências da LGPD quanto ao uso de dados dos colaboradores	☐ Sim ☐ Não ☐ Parcial	
10. Compartilhamento com Terceiros Controlado	Em caso de repasse a clínicas, consultorias ou plataformas digitais, há contrato com cláusulas de proteção de dados?	☐ Sim ☐ Não ☐ Parcial	
11. Treinamento de Envolvidos	Equipes de SST, RH e terceiros foram treinados sobre LGPD e confidencialidade?	☐ Sim ☐ Não ☐ Parcial	
	Existe programa de capacitação contínua sobre segurança e proteção de dados	☐ Sim ☐ Não ☐ Parcial	
	A comunicação interna reforça a importância da privacidade dos trabalhadores?	☐ Sim ☐ Não ☐ Parcial	
	Os treinamentos têm conteúdo, frequência e registros documentais adequados?	☐ Sim ☐ Não ☐ Parcial	
	Há procedimentos para comunicação de acidentes e emissão de CAT?	☐ Sim ☐ Não ☐ Parcial	
	A documentação de SST é mantida organizada e acessível para fiscalização?	☐ Sim ☐ Não ☐ Parcial	
	Existem registros dos treinamentos (listas, certificados, avaliações) ?	☐ Sim ☐ Não ☐ Parcial	
12. Retenção e Eliminação de Dados	Existe política de retenção e descarte seguro de dados, conforme exigência legal (ex: exames mantidos por 20 anos)?	☐ Sim ☐ Não ☐ Parcial	
13. Encarregado (DPO) Nomeado	Há um encarregado de dados (DPO) responsável por atender titulares e a ANPD?	☐ Sim ☐ Não ☐ Parcial	

14. Direitos dos Titulares Atendidos	É possível atender solicitações dos trabalhadores sobre seus dados (acesso, correção, exclusão, etc.)?	☐ Sim ☐ Não ☐ Parcial	
	Os trabalhadores têm canal para exercer seus direitos (acesso, correção, exclusão, etc.)?	☐ Sim ☐ Não ☐ Parcial	
	Existe procedimento para atendimento às solicitações dos titulares?	☐ Sim ☐ Não ☐ Parcial	
	Os titulares são informados em caso de incidente de segurança envolvendo seus dados?	☐ Sim ☐ Não ☐ Parcial	
	Os colaboradores foram envolvidos na identificação de perigos e na avaliação dos riscos	☐ Sim ☐ Não ☐ Parcial	
	Existe um Canal de Denúncia independente e isento? (Fora da Empresa)	☐ Sim ☐ Não ☐ Parcial	
15. Auditorias Periódicas	São feitas auditorias e revisões periódicas da conformidade LGPD no GRO/PGR?	☐ Sim ☐ Não ☐ Parcial	
	Existe registro das atividades de tratamento relacionadas à NR-01	☐ Sim ☐ Não ☐ Parcial	
	As atividades de SST passam por auditoria periódica de conformidade com a LGPD?	☐ Sim ☐ Não ☐ Parcial	
	Incidentes ou não conformidades são documentados e tratados?	☐ Sim ☐ Não ☐ Parcial	
	Existe um Programa de Gerenciamento de Risco - PGR	☐ Sim ☐ Não ☐ Parcial	
16. Governança e Responsabilidade	Existe política de privacidade e proteção de dados aplicada aos dados de saúde e segurança do trabalho	☐ Sim ☐ Não ☐ Parcial	
	O sistema de gerenciamento de riscos considera o ciclo de vida dos dados pessoais?	☐ Sim ☐ Não ☐ Parcial	
17. Coleta e Tratamento de Dados Pessoais	Há mapeamento dos dados pessoais coletados durante os processos da NR-01 (inventário de riscos, PGR, ASO, etc.)?	☐ Sim ☐ Não ☐ Parcial	
	Os trabalhadores são informados sobre quais dados são coletados e por quê?	☐ Sim ☐ Não ☐ Parcial	
	O consentimento é colhido quando necessário (ex: dados não obrigatórios)?	☐ Sim ☐ Não ☐ Parcial	
	Existe controle de acesso e rastreabilidade de quem acessa dados de SST?	☐ Sim ☐ Não ☐ Parcial	
	Existe setores com poucos funcionários e risco de identificação do colaborador ?	☐ Sim ☐ Não ☐ Parcial	

	Existem documentos vencidos ou desatualizados?	☐ Sim ☐ Não ☐ Parcial	
	Há o risco de identificação do titular vinculado à função?	☐ Sim ☐ Não ☐ Parcial	
18. Compartilhamento e Terceirização	Fornecedores ou clínicas terceirizadas que realizam exames ou treinamentos estão em conformidade com a LGPD?	☐ Sim ☐ Não ☐ Parcial	
	Há contratos com cláusulas de proteção de dados com terceiros envolvidos na SST?	☐ Sim ☐ Não ☐ Parcial	
	O compartilhamento de dados com órgãos públicos (ex: eSocial, Ministério do Trabalho) está documentado e justificado legalmente?	☐ Sim ☐ Não ☐ Parcial	

- Marque o status de conformidade (Sim, Não, Parcial).
- Preencha o checklist em conjunto com as áreas de SST, TI, RH, LGPD e jurídico.
- Mantenha este documento arquivado como evidência de conformidade.
- Anote evidências (ex: nome do documento, data do último treinamento).
- Defina ações corretivas com prazos e responsáveis quando necessário

RISCOS QUE A NR01 PODE TRAZER À LGPD

PRIVACIDADE E PROTEÇÃO DE DADOS (LGPD)				
Risco	**Tipo de Dado**	**Consequência Potencial**	**Base Aplicável**	**Medidas de Mitigação**
Coleta excessiva de dados em ASO ou laudos	Sensível (saúde)	Violação de privacidade, processo judicial	Obrigação legal	Limitar coleta ao necessário
Armazenamento físico de documentos sem controle	Sensível	Vazamento, acesso indevido	Obrigação legal	Armário trancado, acesso restrito
Envio de dados de saúde por e-mail sem criptografia	Sensível	Interceptação, uso indevido	Obrigação legal	E-mails criptografados, política de envio
Falta de informação ao trabalhador sobre seus dados	Pessoal/Sensível	Descumprimento da LGPD	Transparência	Avisos e políticas de privacidade claras
Compartilhamento de dados com clínicas terceirizadas sem contrato adequado	Sensível	Responsabilização solidária	Execução de contrato	Contratos com cláusulas de LGPD
Acesso não autorizado a sistemas de SST	Pessoal/Sensível	Vazamento de informações	Legitimo interesse/obrigação legal	Controle de acesso, logs de auditoria
Ausência de canal para exercício dos direitos dos titulares	Pessoal/Sensível	Multas, sanções da ANPD	Direitos do titular	Implantar canal de atendimento
Incidente de segurança sem plano de resposta	Pessoal/Sensível	Sanções, dano à reputação	Art. 46 da LGPD	Plano de resposta a incidentes
Treinamento insuficiente sobre LGPD na equipe de SST	Sensível	Tratamento incorreto de dados	Obrigação do controlador	Capacitação contínua
Publicação de nomes e dados em murais ou sistemas expostos	Pessoal	Exposição indevida, constrangimento	Consentimento (se aplicável)	Uso de identificadores anônimo
RISCOS DE CONFORMIDADE				

Risco	Impacto	Consequência Legal/Regulatória	Ação Recomendável
Ausência de inventário de dados tratados na SST	Alto	Não conformidade com LGPD	Realizar mapeamento de dados
Falta de registro das bases legais utilizadas	Médio	Fragilidade jurídica	Documentar bases legais por processo
Não conformidade em auditorias do PGR/NR-01	Alto	Autos de infração	Acompanhamento e revisão periódica
Ausência de cláusulas LGPD nos contratos de SST terceirizados	Alto	Responsabilidade compartilhada	Readequar contratos
Utilização de softwares de SST sem avaliação de segurança	Alto	Risco de vazamento	Avaliar e validar ferramentas com TI

DOCUMENTOS DE APOIO

Documento	Finalidade	LGPD Relevância	Periodicidade de Revisão
Política de Privacidade Interna	Informar trabalhadores sobre uso de dados	Transparência	Anual
Registro de Tratamento de Dados	Controlar dados coletados no SST	Art. 37	Semestral
Termos de Consentimento (se aplicável)	Uso de dados não obrigatórios	Art. 7º, I	Conforme necessidade
Plano de Resposta a Incidentes	Mitigação de vazamentos	Art. 46	Anual/Testes periódicos
Treinamento LGPD para SST	Capacitação	Art. 6º, X	Semestral/Novos contratados