



MTR-GOV-003

Programa de Privacidade, Estrutura



A estrutura de governança que sustenta a política de proteção de dados: quem responde por quê, os dez pilares do programa, os fluxos de direitos e de incidentes, os indicadores e as evidências que entregamos em due diligence.

CODIGO	VERSAO
MTR-GOV-003	1.0
STATUS	APROVACAO
MINUTA	a definir: data de aprovação pela Direção
RESPONSAVEL	PROXIMA REVISAO
Encarregado pelo Tratamento de Dados Pessoais	12 meses após a aprovação

Minuta. Este documento ainda nao foi aprovado pela Direcao e nao deve ser apresentado em processo de habilitacao ou due diligence enquanto houver campo a definir.

1. Objetivo

Uma política diz o que a empresa se compromete a fazer. Este documento diz **como** esse compromisso é operado, por quem, com que ritmo e com que prova.

Ele descreve o programa de governança em privacidade da Metrion Service, nos termos do artigo 50 da Lei 13.709/2018, e serve de referência para clientes, concessionárias e órgãos que avaliem a nossa maturidade em proteção de dados em processos de qualificação, licitação e auditoria de fornecedor.

2. Escopo

O programa cobre todo tratamento de dados pessoais sob responsabilidade da Metrion, nas duas condições descritas na Política de Proteção de Dados Pessoais (MTR-GOV-002): como controladora dos seus próprios dados de pessoas, candidatos, contatos e visitantes, e como operadora do cliente gerador nos dados que trata por conta dele dentro do contrato de serviço.

Cobre também os terceiros que tratam dados em nome da Metrion, na medida da relação contratual.

3. Estrutura de governança

3.1 Direção

Aprova o programa e a política, define o apetite a risco, provê recursos e orçamento, recebe o relatório periódico do Encarregado e responde institucionalmente pela conformidade.

3.2 Encarregado pelo Tratamento de Dados Pessoais

Indicado formalmente pela Direção, com identidade e contato divulgados publicamente no site, conforme exige o artigo 41 da LGPD.

Atribuições:

- ser o canal com titulares, clientes controladores e ANPD;
- manter o inventário de operações de tratamento e o registro exigido pelo artigo 37;
- orientar as áreas antes do início de tratamento novo;
- conduzir o fluxo de direitos de titulares e o de incidentes;
- propor e acompanhar o plano de adequação;
- reportar o estado do programa à Direção;
- guardar as evidências que sustentam o programa.

O Encarregado tem acesso direto à Direção e independência para reportar não conformidade sem filtro da área envolvida.

- Encarregado indicado: *a definir: nome, cargo, e-mail e ato de designação do Encarregado*

3.3 Comitê de Privacidade e Segurança da Informação

Fórum de decisão, com reunião ordinária trimestral e extraordinária sempre que houver incidente relevante.

Composição mínima sugerida: Encarregado, representante da Direção, responsável por Tecnologia da Informação, responsável por Gente e Gestão, responsável por Operações e apoio jurídico.

- Composição aprovada: *a definir: composição nominal do Comitê de Privacidade e Segurança da Informação*

Pauta permanente: pedidos de titulares e prazos, incidentes e ações, andamento do plano de adequação, riscos abertos, mudanças legais e regulatórias, avaliação de terceiros.

3.4 Gestores de processo

Cada área que trata dados pessoais tem um responsável nomeado, que mantém o seu trecho do inventário atualizado, garante o treinamento da equipe e aciona o Encarregado antes de criar um tratamento, contratar uma ferramenta ou iniciar um projeto que envolva dados pessoais.

3.5 Todas as pessoas

Cumprem a política, acessam somente o necessário à função, protegem credenciais e comunicam incidente ou suspeita imediatamente.

4. Ciclo do programa

O programa opera em ciclo contínuo, com revisão anual completa:

Mapear as operações de tratamento e os fluxos de dados. → **Avaliar** riscos e lacunas frente à LGPD e aos contratos. → **Tratar** as lacunas com plano de ação, prazo e responsável. → **Operar** as rotinas de direitos, incidentes, acessos e terceiros. → **Monitorar** por indicadores, testes e auditoria. → **Melhorar** com lição aprendida e atualização da documentação.

5. Os dez pilares

Pilar 1, Inventário de operações de tratamento

Registro vivo de todas as operações, contendo: processo, finalidade, base legal, categorias de titulares e de dados, origem, sistemas envolvidos, compartilhamentos, transferência internacional, prazo de retenção, medidas de segurança e responsável.

Atualização obrigatória a cada nova operação e revisão consolidada semestral.

Pilar 2, Bases legais e avisos de privacidade

Toda operação tem base legal definida e documentada. As avaliações de legítimo interesse são registradas por escrito, com a ponderação feita e as mitigações adotadas.

Avisos de privacidade específicos e atualizados existem para: site e formulários, processos seletivos, admissão e relação de trabalho, fornecedores, e controle de acesso e monitoramento por vídeo em instalações da Metrion.

MTR-GOV-003 V1.0 MINUTA

METRION SERVICE DOCUMENTO CONTROLADO

Pilar 3, Direitos dos titulares

Canal único, prazos controlados e registro de cada pedido. Fluxo detalhado na seção 6.

Pilar 4, Gestão de terceiros

Nenhum fornecedor que trate dados pessoais é contratado sem avaliação prévia e sem cláusula de proteção de dados no contrato.

O que a cláusula precisa prever: finalidade e instruções, vedação de uso próprio, confidencialidade, medidas de segurança, regime de subcontratação, auxílio no atendimento a titulares, comunicação imediata de incidente, direito de auditoria, e devolução ou eliminação ao término.

Nos contratos em que a Metrion é operadora, o espelho dessas obrigações é assumido por nós perante o cliente controlador.

Reavaliação dos fornecedores críticos: anual.

Pilar 5, Segurança da informação

Controles mínimos exigidos, aplicados conforme a criticidade do sistema:

- identidade individual, senha forte e segundo fator onde houver suporte;
- acesso por perfil, concedido por necessidade, revisado semestralmente e revogado no dia do desligamento;
- criptografia em trânsito, e em repouso onde aplicável;
- backup com teste de restauração periódico;
- registro de acesso e trilha de auditoria nos sistemas críticos;
- gestão de vulnerabilidades e atualização de sistemas;
- segregação entre bases de clientes distintos;
- controles próprios para campo: cifragem de disco, bloqueio de tela, gestão de dispositivo móvel, apagamento remoto, regras de fotografia e de uso de drone;
- descarte seguro de papel e sanitização de mídia.

Pilar 6, Gestão de incidentes

Procedimento escrito, com papéis, prazos e modelos de comunicação. Fluxo detalhado na seção 7. Teste de mesa ao menos uma vez por ano.

Pilar 7, Relatório de Impacto à Proteção de Dados Pessoais

O RIPD é obrigatório antes de iniciar tratamento de risco elevado. Gatilhos que exigem RIPD na Metrion:

- monitoramento por vídeo com captação de pessoas;

- geolocalização de equipes ou de veículos;

MTR-CCV-005 - V1.0 - MINUTA METRION SERVICE DOCUMENTO CONTROLADO

- tratamento de dado biométrico, inclusive para controle de jornada;
- tratamento de dado sensível fora das rotinas ocupacionais já mapeadas;
- uso de imagens aéreas capazes de identificar pessoas;
- decisão automatizada com efeito sobre uma pessoa;
- tratamento em larga escala de dados de terceiros a pedido do cliente.

O RIPD é aprovado pelo Encarregado antes da entrada em produção e revisado quando o tratamento mudar.

Pilar 8, Treinamento e cultura

- Módulo de privacidade na integração de toda pessoa admitida, com registro.
- Reciclagem anual para todos.
- Treinamento dirigido às funções de maior exposição: Tecnologia da Informação, Gente e Gestão, comercial, contratos, coordenação de campo e liderança.
- Comunicação periódica com casos práticos do nosso dia a dia, incluindo simulação de phishing.

Pilar 9, Monitoramento e auditoria

Indicadores acompanhados pelo Comitê, revisão semestral de acessos, teste anual de restauração de backup, simulação anual de incidente e auditoria interna do programa ao menos uma vez por ano.

Não conformidade encontrada vira plano de ação com responsável e prazo, acompanhado até o encerramento.

Pilar 10, Documentação e evidências

Todo pilar produz evidência guardada e recuperável. É esse acervo que responde a questionário de cliente, a due diligence de concessionária e a eventual requisição da ANPD. A lista está na seção 10.

6. Fluxo de direitos dos titulares

1. **Entrada.** O pedido chega pelo canal de privacidade e é protocolado no mesmo dia útil, com data, identificação do titular, direito exercido e prazo final.
2. **Verificação de identidade.** Confirmação proporcional ao risco, usando os dados apenas para essa finalidade.
3. **Classificação.** O Encarregado define se a Metrion é controladora ou operadora nesse caso.
4. **Se operadora:** encaminhamento ao cliente controlador em até 2 dias úteis, com aviso ao titular, e execução do que o controlador instruir.
5. **Se controladora:** localização dos dados nos sistemas mapeados pelo inventário, análise de cabimento e de eventual dever legal de conservação.

6. **Resposta.** Em formato simplificado de imediato, ou completa em até 15 dias da requisição. Recusa é sempre fundamentada e informa o direito de reclamar à ANPD.
-
7. **Registro.** Pedido, análise, resposta e comprovante de envio ficam arquivados como evidência.

7. Fluxo de incidentes

1. **Deteção e comunicação interna.** Quem percebe comunica o Encarregado imediatamente, por qualquer meio, sem análise prévia.
2. **Registro.** Abertura de ocorrência com data e hora de conhecimento, que é o marco de contagem dos prazos.
3. **Contenção.** Interrupção do acesso indevido, bloqueio de credencial, isolamento de máquina, revogação de link, apagamento remoto.
4. **Avaliação de risco.** Natureza e volume dos dados, titulares afetados, possibilidade de identificação, gravidade da consequência possível, medidas de segurança que já protegem os dados.
5. **Acionamento.** Comitê convocado. Cliente controlador comunicado imediatamente quando os dados forem dele. Jurídico e seguro acionados conforme o caso.
6. **Comunicação externa.** Se houver risco ou dano relevante, comunicação à ANPD e aos titulares no prazo da regulamentação vigente, hoje de 3 dias úteis do conhecimento, com a descrição dos dados, dos titulares, das medidas técnicas de proteção, dos riscos e das providências adotadas.
7. **Correção e lição aprendida.** Causa raiz, plano de ação, atualização de controle e de treinamento, revisão do procedimento.

8. Matriz de responsabilidades

MTR-GOV-003 V1.0 MINUTA	METRION SERVICE DOCUMENTO CONTROLADO				
Atividade	Direção	Encarregado	Comitê	TI	Gestor de área
Aprovar política e programa	Aprova	Propõe	Consultado	Consultado	Informado
Manter inventário de tratamentos	Informada	Responsável	Informado	Apoia	Executa no seu escopo
Atender direito de titular	Informada	Responsável	Informado	Apoia	Apoia
Responder a incidente	Informada	Coordena	Decide	Executa contenção	Apoia
Avaliar fornecedor	Informada	Define critério	Consultado	Avalia técnica	Executa
Elaborar RIPD	Informada	Aprova	Consultado	Apoia	Elabora
Treinar equipes	Patrocina	Define conteúdo	Acompanha	Apoia	Garante presença
Auditar o programa	Recebe relatório	Coordena	Avalia	Apoia	Atende

9. Indicadores do programa

Acompanhados pelo Comitê a cada trimestre, com data-base declarada em todo reporte:

- percentual de operações de tratamento inventariadas e revisadas no período;
- número de pedidos de titulares recebidos, atendidos e atendidos dentro do prazo;
- número de incidentes registrados, contidos e comunicados no prazo;
- percentual de pessoas treinadas na integração e na reciclagem anual;
- percentual de fornecedores críticos com cláusula de proteção de dados assinada;
- percentual de acessos revisados no ciclo semestral;
- ações do plano de adequação concluídas no prazo;
- resultado do teste anual de restauração de backup e da simulação de incidente.

10. Evidências disponíveis para clientes, licitações e auditorias

Este é o acervo que a Metrion mantém e apresenta quando um contratante avalia o nosso programa:

- Código de Ética e Conduta vigente, com termo de adesão assinado pelas equipes;
- Política de Proteção de Dados Pessoais vigente;
- este documento de estrutura do programa;

- ato de designação do Encarregado, com contato público;

MTR-GOV-003 V1.0 MINUTA METRION SERVICE DOCUMENTO CONTROLADO

- inventário de operações de tratamento, apresentado de forma resumida quando houver informação sensível ao negócio;

- avaliações de legítimo interesse e RIPDs realizados;
- procedimento de resposta a incidentes e registro do último teste;
- registros de treinamento por período;
- modelo de cláusula de proteção de dados usado com fornecedores;
- relação de subcontratados relevantes que tratam dados, e das transferências internacionais;
- registros de atendimento a titulares, anonimizados;
- último relatório de auditoria interna do programa e o respectivo plano de ação;
- apólices e certificados aplicáveis: *a definir: relação de apólices e certificados que a Metrion apresenta em habilitação*.

11. Calendário anual

Período	Atividade
Janeiro	Revisão de acessos, primeiro ciclo
A cada trimestre	Reunião do Comitê e reporte de indicadores à Direção
Abril	Reavaliação de fornecedores críticos
Junho	Revisão consolidada do inventário, primeiro ciclo
Julho	Simulação de incidente e teste de restauração de backup
Setembro	Reciclagem anual de treinamento
Outubro	Auditoria interna do programa
Novembro	Revisão dos documentos MTR-GOV-001, 002 e 003
Dezembro	Revisão de acessos, segundo ciclo, e revisão do inventário

12. Plano de adequação

O estado atual do programa e as ações em curso são acompanhados em plano próprio, com responsável e prazo por ação, revisado no Comitê.

Ações estruturantes ainda pendentes nesta versão: *a definir: designação formal do Encarregado, contratação do Canal de Ética, conclusão do inventário de tratamentos e assinatura das cláusulas de proteção de dados com fornecedores críticos*.

Enquanto a designação do Encarregado não for publicada, os contatos de privacidade são respondidos pela Direção da Metrion Service.

MTR-GOV-003 V1.0 MINUTA

METRION SERVICE DOCUMENTO CONTROLADO

13. Vigência e revisão

Este documento entra em vigor na data da sua aprovação, com revisão a cada 12 meses ou sempre que houver alteração legal, regulatória, contratual ou organizacional relevante.

A versão vigente é a publicada na seção de Governança e Compliance do site da Metrion. Cópias impressas ou salvas localmente são cópias não controladas.