CRM-TO

CONSELHO REGIONAL DE MEDICINA DO ESTADO DO TOCANTINS

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

Versão 1.1

25/11/2021

SUMÁRIO

INTRODUÇÃO

A Lei n° 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) é a legislação brasileira que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A LGPD tem como fundamentos o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A LGPD, em sua Seção II, Das Boas Práticas e da Governança, no art. 50, § 2°, I, determina que o controlador, a quem competem as decisões referentes ao tratamento de dados pessoais, poderá implementar programa de governança em privacidade que, no mínimo:

a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;

c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

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

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;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

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

O CRM/TO, assim como todos os demais órgãos e entidades da Administração Pública que coletam e tratam dados para o fornecimento de seus serviços, deve se adequar à LGPD. Inicialmente, essa adequação envolve uma transformação cultural que abrange os níveis estratégico, tático e operacional da instituição.

Adicionalmente, considera a privacidade dos dados pessoais do cidadão desde a fase de concepção do serviço ou produto até sua execução (Privacidade by Design) e promover ações de conscientização de todo corpo funcional, no sentido de incorporar o respeito à privacidade dos dados pessoais nas atividades institucionais cotidianas.

Assim, o presente documento apresenta o Programa de Governança em Privacidade a ser implementado pelo CRM/TO (PGP-CRM/TO). O Programa será atualizado e ampliado sempre que necessário para manter alinhamento com as diretrizes determinadas pela Autoridade Nacional de Dados Pessoais (ANPD).

O PGP-CRM/TO está em consonância com o Guia de Elaboração de Programa de Governança em Privacidade da Secretaria de Governo Digital do Ministério da Economia (SGD/ME).

O presente Programa leva em consideração a estrutura organizacional do CRM/TO e suas especificidades. O PGP-CRM/TO atua de forma complementar e adicional às ações já em andamento e não visa substituir demais documentos e atos normativos que disponham sobre o tratamento de dados no âmbito do CRM/TO.

OBJETIVO

O PGP-CRM/TO tem o objetivo de garantir a proteção de dados e a privacidade dos cidadãos em todas as etapas de desenvolvimento de seus processos de trabalho, internos e externos.

ETAPAS

O PGP-CRM/TO visa centralizar as ações realizadas ou em andamento e disponibilizar uma visão geral da adequação do CRM/TO à LGPD. Para isso, ele consiste na captura e consolidação dos requisitos de privacidade e segurança exigidos pela LGPD, de

forma a ditar e influenciar como os dados pessoais são manuseados no seu ciclo de vida como um todo.

Sua elaboração foi realizada com base nos seguintes marcos de conformidade com a LGPD:

1) Programa de Privacidade;
2) Inventário de tratamento de dados;
3) Termos de uso e política de privacidade;
4) Adequação de contratos;
5) Relatório de impacto de proteção de dados;
6) Resposta a incidentes;
7) Publicação no Portal da Transparância do CRM/TO.

A estrutura do PGP-CRM/TO é inspirada no ciclo PDCA, bem como nas normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27701:2019. Tecnologia da Informação - Técnicas de Segurança – Código de Prática para controles de segurança da informação e ABNT NBR ISO/IEC 27005:2011. Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação, conforme orientação do Guia de Elaboração de Programa de Governança em Privacidade da SGD/ME.

O PGP-CRM/TO será executado em três etapas, conforme abaixo:

ETAPA 1: Iniciação e Planejamento

A etapa de Iniciação e Planejamento busca compreender quais são as primeiras informações e os dados que devem ser conhecidos.

De acordo com o Guia de Elaboração de Programa de Governança em Privacidade da SGD/ME, esta etapa consiste nos seguintes marcos:

MARCO 1: Nomeação do Encarregado;

MARCO 2: Alinhamento de expectativas com a Alta Administração;

MARCO 3: Análise da maturidade - Diagnóstico do atual estágio de adequação à LGPD;

MARCO 4: Análise e adoção de medidas de segurança, diretrizes e cultura interna;

MARCO 5: Instituição de estrutura organizacional para a governança e gestão da proteção de dados pessoais;

MARCO 6: Inventário de Dados Pessoais (IDP);

MARCO 7: Levantamento dos contratos relacionados à dados pessoais.

MARCO 1: Nomeação do Encarregado

De acordo com o art 5°, VIII, da LGPD, o Encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.

A Portaria CRM-TO nº 41/2021 designou o Advogado do CRM/TO Wesley Monteiro de Castro Neri como Encarregado pelo tratamento de dados pessoais e para o exercício das seguintes atribuições:

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

II - receber comunicações da ANPD 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;

IV - Apoiar a definição das diretrizes de construção do inventário de dados pessoais relativas ao registro das operações de tratamento de dados pessoais determinadas pelo art. 37 da LGPD;

V - Conduzir ou aconselhar a elaboração de relatório de impacto à proteção de dados pessoais, de acordo com os casos previstos pela LGPD em que tal documento é necessário;

VI - Conduzir ou aconselhar a implementação de regras de boas práticas e de governança especificadas pelo art. 50 da LGPD;

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

A LGPD estabelece que a ANPD poderá estabelecer normas complementares sobre a definição e as atribuições do Encarregado.

Os dados do Encarregado estão públicos e acessíveis no sítio eletrônico pelo link <https://transparencia.crmto.org.br/index.php/2021-06-18-11-53-07/protecao-de-dados-pessoais>.

MARCO 2: Alinhamento de Expectativas com a Alta Administração

A LGPD apresenta, em seu art 5°, os principais atores envolvidos na adequação dos órgãos e entidades à LGPD:

- Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
- Agentes de tratamento: o controlador e o operador;

- Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD;
- Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

A participação da alta administração, representando o papel do controlador, é crucial para a efetividade das ações relacionadas ao cumprimento das obrigações estipuladas pela LGPD, bem como para o sucesso do trabalho executado pelo Encarregado, incluindo seu envolvimento nas decisões e recursos para pessoal, treinamento, entre outros.

A Instrução Normativa CFM nº 003/2021 garante ao Encarregado acesso direto à Alta Administração para alinhar com o Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais as etapas da adequação à LGPD que serão priorizadas.

MARCO 3: Análise da Maturidade - Diagnóstico do Atual Estágio de Adequação à LGPD

Em novembro de 2021, o Encarregado realizou o diagnóstico de maturidade do CRM/TO e índice de adequação à LGPD por meio de formulário disponibilizado pela SGD/ME no site <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/diagnostico-privacidade-lgpd>.

As respostas subsidiaram análise que possibilitou o direcionamento de esforços e a priorização das ações necessárias para construção da conformidade à lei de proteção de dados.

De acordo com o referido formulário, a maturidade do CRM/TO estava em estágio inicial, carecendo de padrões para transparência e comunicação com o cidadão, tais como termos de uso, canal de comunicação amplamente divulgado para tratar de dados pessoais, entre outros. O cálculo do índice de adequação à LGPD está demonstrado na tabela abaixo:

Dimensões	Índice	Nível
1 - Dimensão Governança	0.51	
2 - Dimensão Conformidade legal e respeito aos princípios	0.23	
3 - Dimensão Transparência e direitos do titular	0.42	
4 - Dimensão Rastreabilidade	0.2	
5 - Dimensão Adequação de contratos e de relações com parceiros	0.2	
6 - Dimensão Segurança da Informação	0.08	
7 - Dimensão Violações de Dados	0.29	
Índice da Adequação à LGPD	**0.28**	**Inicial**

A avaliação do nível de maturidade do CRM/TO será realizada recorrentemente, de forma a atuar como um índice de performance, e divulgada na etapa de Monitoramento do PGP-CRM/TO.

MARCO 4: Análise e Adoção de Medidas de Segurança, Diretrizes e Cultura Interna

Em seu art. 46, a LGPD determina que os agentes de tratamento devem adotar medidas de segurança, técnicas e ações 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. O § 2º do mesmo artigo dispõe que tais medidas deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução, conforme o conceito de Privacidade desde a Concepção (do inglês Privacy by Design).

Assim, as ações realizadas e as documentações produzidas pelo CRM/TO para adequação à LGPD, tais como o presente PGP-CRM/TO, o Inventário de Dados Pessoais - IDP, os Termos de Política de Uso e Privacidade, o Levantamento dos Riscos de Segurança e Privacidade, a adequação dos Contratos, o Relatório de Impacto de Proteção dos Dados, o

Plano de Resposta a Incidentes, bem como outros documentos internos, serão construídos tendo por base o conceito de Privacy by Design.

MARCO 5: Instituição de Estrutura Organizacional para a Governança e Gestão de Proteção de Dados Pessoais

O CRM/TO, por meio da PORTARIA CRM-TO nº 40/2021, 17 de Junho de 2021, instituiu o Comitê Gestor de Segurança da Informação e Proteção de Dados Pessoais, de caráter permanente, natureza deliberativa e tipo estratégico.

A finalidade do Comitê é prestar suporte aos trabalhos da LGPD, sendo formado por uma equipe técnica e multidisciplinar, que desempenhe as funções jurídica, de segurança da informação e tecnológica, de comunicação interna e externa, de recursos humanos, de gestão documental e estratégica.

O Comitê Gestor é composto pelos seguintes membros:

- Presidente do CRM/TO;
- 1º Secretário do CRM/TO;
- Gerente administrativo;
- Chefe do Setor de TI;
- Assessor de comunicação.

MARCO 6: Inventário de Dados Pessoais (IDP)

De acordo com o art. 37 da LGPD, o IDP consiste no registro das operações de tratamento dos dados pessoais realizados pela instituição e deverá descrever informações tais como:

- atores envolvidos (agentes de tratamento e o Encarregado);
- finalidade (o que a instituição faz com o dado pessoal);
- hipótese (arts. 7° e 11 da LGPD);

- previsão legal;
- dados pessoais tratados pela instituição;
- categoria dos titulares dos dados pessoais;
- tempo de retenção dos dados pessoais;
- instituições com as quais os dados pessoais são compartilhados;
- transferência internacional de dados (art. 33 da LGPD); e
- medidas de segurança atualmente adotadas.

O IDP é um importante documento de governança, fornecendo subsídios para avaliação de impacto à proteção de dados pessoais, com vistas a verificar a conformidade da instituição à LGPD, pois permite identificar áreas-chave, papéis e responsabilidades para o PGP.

Sua elaboração deve levar em conta o ciclo de vida dos dados, ou seja, coleta, uso, transferências, retenção e destruição, bem como deve contemplar, idealmente, todas as atividades de tratamento previstas na LGPD.

O IDP do CRM/TO encontra-se em elaboração e baseia-se na metodologia sugerida pelo Guia de Elaboração de Inventário de Dados Pessoais da SGD/ME (https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf).

MARCO 7: Levantamento os Contratos Relacionados a Dados Pessoais

Ao realizar o levantamento dos serviços que tratam dados pessoais, o IDP viabiliza a correlação com os contratos que os suportam. O mapeamento destes contratos que coletam, transferem e processam dados pessoais contribui para a análise de possíveis e necessárias adequações, tanto nos existentes, quanto nos futuros.

Para esse passo, o CRM/TO se baseará no Guia de Adequação de Contratos (https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_requisitos_obrigacoes.pdf) para elaborar cláusulas que assegurem a proteção dos dados pessoais, tanto nos novos contratos como nas renovações dos vigentes.

ETAPA 2: Construção e Execução

A presente etapa trata da implementação propriamente dita do PGP-CRM/TO por meio dos seguintes marcos:

MARCO 1: Políticas e práticas para a proteção da privacidade ao cidadão;
MARCO 2: Cultura de segurança e proteção de dados e Privacy by Design;
MARCO 3: Relatório de Impacto à Proteção de Dados Pessoais (RIPD);
MARCO 4: Política de Privacidade e Política de Segurança da informação;
MARCO 5: Termo de Uso;
MARCO 6: Adequação de cláusulas contratuais;
MARCO 7: Plano de Capacitações e Comunicações.

MARCO 1: Políticas e práticas para a proteção da privacidade ao cidadão

Um PGP contém políticas e práticas que visem proteger a privacidade do cidadão, garantindo que todos os usos dos dados pessoais sejam conhecidos e adequados às leis, bem como haja proteção contra mau uso ou revelação inadvertida ou deliberada.

Adicionalmente, a Administração Pública deve assegurar o exercício das atividades específicas dos servidores envolvidos na coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais. Deve também fomentar a educação dos colaboradores em relação a políticas e práticas de proteção à privacidade, e, complementarmente, dos cidadãos, em relação aos direitos de privacidade.

Atualmente, o Plano de Resposta a incidentes, a Política de Privacidade e a Política de Segurança da Informação encontram-se em fase de planejamento.

MARCO 2: Cultura de segurança e proteção de dados e Privacy by Design

Conforme o art. 46 da LGPD, a proteção dos dados pessoais é alcançada por meio de medidas de segurança e técnicas administrativas, que deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Como custodiante e responsável pelo tratamento de dados pessoais coletados e processados por meio dos serviços internos e externos que oferece, o CRM/TO possui obrigação de assegurar a segurança da informação e proteção destes dados.

De acordo com o Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD), para Implementação na Administração Pública Federal, tal privacidade pode ser alcançada por meio da aplicação dos 7 Princípios Fundamentais (Cavoukian, 2009), listados a seguir:

1. **Proativo, e não reativo; preventivo, e não corretivo:** o conceito de Privacy by Design se caracteriza por medidas proativas e não reativas, visando impedir a ocorrência dos riscos de privacidade, sem esperar que estes se materializem ou oferecer soluções para as infrações de privacidade após a ocorrência;
2. **Privacidade deve ser o padrão dos sistemas de TI ou práticas de negócio:** o objetivo é oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou prática de negócios, sem que seja necessária qualquer ação por parte do titular dos dados, pois ela já estará embutida no sistema, por padrão;
3. **Privacidade incorporada ao projeto (design):** objetiva que a privacidade se torne um componente essencial da funcionalidade principal a ser entregue, sendo parte integrante do sistema, sem diminuir a funcionalidade;
4. **Funcionalidade total:** a incorporação da privacidade em uma determinada tecnologia, processo ou sistema, deve ser realizada de forma a não comprometer a plena funcionalidade e permitir que todas as exigências do projeto sejam atendidas;

5. **Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados:** conforme disposto no art. 6°, VII, segurança é a 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. Sem segurança forte, não pode haver privacidade. Assim, as instituições devem assumir a responsabilidade pela segurança dos dados pessoais, geralmente proporcional ao grau de sensibilidade, durante todo o ciclo de tratamento, consistente com os padrões que foram definidos por organismos reconhecidos de desenvolvimento de padrões;
6. **Visibilidade e Transparência:** por serem valores essenciais para o estabelecimento de responsabilidade e confiança, sua avaliação deve concentrar-se, especialmente, em aspectos como responsabilização, abertura e conformidade.
7. **Respeito pela privacidade do usuário:** é alcançado por meio de medidas como padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que empoderem o titular dos dados. É suportado pelos seguintes aspectos: consentimento ou hipótese de tratamento prevista em lei; precisão; acesso; e conformidade.

MARCO 3: Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

O RIPD é documento fundamental para demonstrar que o controlador realizou uma avaliação dos riscos nas operações de tratamento de dados pessoais e quais medidas são adotadas para sua eventual mitigação.

O RIPD descreve os 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. Deve conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Nem toda atividade enseja a necessidade de um RIPD e a LGPD deixou em aberto para a ANPD determinar hipóteses em que este relatório será necessário. Assim, o CRM/TO o elaborará quando observar que determinado projeto desenvolvido tenha potencial de alto risco para os direitos e liberdades dos indivíduos, ou quando solicitado pela ANPD ou pelo Encarregado.

MARCO 4: Política de Privacidade e Política de Segurança da Informação

Para a atualização das diretrizes internas de proteção de dados pessoais, deve ser verificado se não há tratamento excessivo de dados, se os controles de segurança são suficientes, se é necessário a retenção de determinados dados tratados e, por fim, se é necessário revisar contratos.

Desse modo, o desenvolvimento de uma política de segurança da instituição é obrigatória para todos os órgãos, conforme disposto no art. 9° da Instrução Normativa n° 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Conforme o Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos, a Política de Privacidade é um documento informativo pelo qual o

prestador de serviço transparece ao usuário a forma como o serviço realiza o tratamento dos dados pessoais e fornece privacidade ao usuário.

O documento é, ao mesmo tempo, um dever do controlador e um direito do titular. O serviço deve informar ao titular do dado como ele fornece a privacidade necessária para que a confidencialidade dos dados prestados seja garantida de forma eficiente e como os princípios abaixo são atendidos:

Finalidade	Adequação
Necessidade	Livre Acesso
Transparência	Qualidade
Segurança	Prevenção
Não discriminação	Responsabilização e Prestação de Contas

Em caso de alguma mudança na operação dos dados ser realizada, ela deve ser comunicada ao titular de forma transparente e deve estar presente na Política de Privacidade do serviço.

Atualmente, encontra-se em elaboração o Termo de Uso e Política de Privacidade.

MARCO 5: Termo de Uso

Conforme o Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos, publicado pela SGD, o Termo de Uso é um documento que fornece uma descrição detalhada do serviço, das condições e das regras aplicáveis a ele.

Ele objetiva a transparência do controlador e operador para com o titular de dados pessoais, comunicando como as atividades de tratamento desses dados observam os princípios dispostos no art. 6° da LGPD.

Ainda conforme o referido Guia, são tópicos que devem constar no Termo de Uso:

- Aceitação dos Termos e Políticas
- Definições

- Arcabouço Legal
- Descrição do serviço
- Direitos do usuário
- Responsabilidades do usuário e da Administração Pública
- Mudanças no Termo de Uso
- Informações para contato
- Foro

O Termo de Uso do CRM/TO deverá ser periodicamente atualizado, de forma que possa refletir, de modo claro e preciso, as finalidades de coleta, uso, armazenamento, tratamento e proteção dos dados pessoais dos titulares, que comumente serão utilizados no exercício de suas competências legais.

Atualmente, encontra-se em elaboração o Termo de Uso e Política de Privacidade.

MARCO 6: Adequação de cláusulas contratuais

Este marco possui o escopo de adaptar os contratos, convênios e outros instrumentos que impliquem no tratamento de dados pessoais, mapeados na etapa de Iniciação e Planejamento. Está diretamente relacionado à IDP e ao levantamento dos contratos relacionados a dados pessoais.

Com base no princípio da Transparência, delineado no art. 6° da LGPD, é importante que os contratos firmados apresentem informações claras e objetivas, abordando, se pertinente:

- Delimitações claras e objetivas das responsabilidades do controlador e operador;
- A forma que é realizada a coleta e o tratamento de dados;
- A existência da possibilidade de o titular acessar os seus dados coletados;
- A forma que é realizada a correção, bloqueio ou eliminação de dados mediante solicitação do titular;

- A existência da possibilidade de revogação do consentimento dado pelo titular;
- O detalhamento de quem tem acesso aos dados, o responsável por seu uso e tratamento, a forma de armazenamento e as particularidades de possíveis auditorias;
- As medidas de proteção e segurança dos dados coletados e armazenados pela contratada.

Para esse marco, o CRM/TO, com o apoio do Setor Jurídico e Setor de Compras e Contratos, construirá cláusulas que protejam os dados pessoais nos contratos futuros e nas renovações de contratos vigentes. Adicionalmente, serão incorporados aos Termos de Referência e demais documentos relacionados, itens que propiciem a proteção de dados pessoais, quando necessários.

MARCO 7: Plano de Capacitações e Comunicações

A implementação ampla e inclusiva do PGP-CRM/TO pressupõe o alinhamento interno de suas etapas, objetivos e ações. Assim, faz-se importante o estabelecimento de um Plano de Capacitações e de Comunicações que seja capaz de realizar treinamento e conscientização do corpo funcional, bem como de informar leis e políticas aplicáveis e as consequências por violá-las, identificar possíveis violações, entre outros aspectos.

O Plano de Capacitações e Comunicações do CRM/TO deverá conter métodos de treinamento e conscientização diversos, tais como cursos de capacitação presenciais ou à distância, reuniões de equipe, boletins informativos, e-mails, informações disponibilizadas no portal eletrônico, entre outros.

Adicionalmente, as campanhas de conscientização deverão ser continuamente desenvolvidas com o apoio da Assessoria de Comunicação do CRM/TO, de forma a desenvolver a cultura da privacidade dentro da instituição.

ETAPA 3: Monitoramento

O Monitoramento permanecerá após a implementação do Programa de Governança em Privacidade, para garantir seu aprimoramento contínuo e a implementação dos marcos abaixo identificados:

MARCO 1: Indicadores de Performance;
MARCO 2: Gestão de Incidentes;
MARCO 3: Análise e Reporte de resultados;

MARCO 1: Indicadores de Performance

Os Indicadores de Performance (Key Performance Indicator - KPI) incluem a análise regular dos principais indicadores de desempenho para verificar lacunas no PGP-CRM/TO, assim como o status de outras iniciativas de privacidade.

O CRM/TO usará inicialmente os indicadores recomendados pela SGD/ME:

- Monitoramento e acompanhamento do número de incidentes de violação de dados pessoais e/ou vazamento de dados pessoais;
- Resultados do Diagnóstico de Adequação à LGPD - índice de adequação;
- Índice de serviços com dados pessoais inventariados: número de serviços com dados pessoais inventariados / número de serviços com dados pessoais do órgão * 100;
- Índice de serviços com termo de uso elaborado: quantidade de serviços com termo de uso elaborado / quantidade de serviços do órgão * 100;
- Índice de serviços com RIPD elaborado: quantidade de serviços com RIPD elaborado / quantidade de serviços do órgão * 100;
- Índice de conscientização em segurança: quantidade de treinamentos realizados / quantidade de treinamentos previstos * 100;

- Índice de quantidade de controles de segurança e privacidade implementados para um determinado serviço: quantidade de controles de segurança e privacidade implementados para um determinado serviço / quantidade total de controles de segurança e privacidade identificados para o serviço * 100.

MARCO 2: Gestão de Incidentes

Um processo de Gestão de Incidentes contempla o registro dos incidentes de segurança da informação e de privacidade ocorridos e onde serão armazenadas as informações: a descrição dos incidentes ou eventos; as informações e sistemas envolvidos; as medidas técnicas e de segurança utilizadas para a proteção das informações; os riscos relacionados ao incidente; e as medidas tomadas para mitigação, a fim de evitar reincidências.

O Plano de Resposta a Incidentes do CRM/TO encontra-se em fase de planejamento, conforme Guia de Resposta a Incidentes de Segurança, publicado pela SGD, e seu endereço será adicionado a uma versão posterior deste PGP-CRM/TO.

MARCO 3: Análise e Reporte de resultados

A análise e divulgação da evolução das ações e dos resultados obtidos são primordiais para o reforço e o fortalecimento da cultura de privacidade dos dados.

Assim, o CRM/TO disponibilizará as referidas informações no Portal da Transparência, por meio do endereço https://transparencia.crmto.org.br, bem como reportará à Diretoria as ações realizadas e resultados obtidos com o PGP-CRM/TO.

CONCLUSÃO

A Lei n° 13.709, de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) tem como objetivo assegurar a proteção à privacidade, a transparência, o desenvolvimento

econômico e tecnológico, a padronização de normas, a segurança jurídica e o favorecimento à concorrência e a livre atividade econômica.

O CRM/TO, na aplicação dos princípios de segurança e prevenção indicados nos incisos VII e VIII do caput do art. 6° da LGPD, e observando sua estrutura, escala e volume de suas operações, bem como a sensibilidade dos dados tratados e probabilidade e gravidade dos danos para os titulares dos dados, apresenta aqui os passos para o processo de implementação do Programa de Governança em Privacidade na Escola (PGP-CRM/TO).

O PGP-CRM/TO consolidou as atividades que visam garantir a proteção à privacidade e o cuidado adequado com os dados coletados e tratados. Existe o entendimento de que o Programa deverá ser atualizado e ampliado permanentemente, de forma a retratar o amadurecimento e desafios institucionais, observando sempre o alinhamento com as diretrizes determinadas pela ANPD.