PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

MPF
Ministério Público Federal

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

MINISTÉRIO PÚBLICO FEDERAL

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

Brasília
MPF
2025

Dados Internacionais de Catalogação na Publicação (CIP)

B823r

Brasil. Ministério Público Federal

Programa de governança em privacidade – Brasília : MPF, 2025.

29 p.

Disponível em: http://hdl.handle.net/11549/317909

1. Proteção de dados pessoais 2. Ministério Público Federal - planejamento. 3.Governança pública. I . Título

CDDir 341.2738

Elaborado por Gisele Bornacki Costa – CRB1/2076

COORDENAÇÃO E ORGANIZAÇÃO
Unidade de Proteção de Dados Pessoais (UPDP)

Encarregado de Proteção de Dados Pessoais
Leonardo Andrade Macedo

Secretaria Executiva
Rita de Cássia Bezerra de Menezes
Débora Raposo Amaral

PLANEJAMENTO VISUAL E DIAGRAMAÇÃO
Secretaria de Comunicação Social (Secom)

Diagramação
Marina Cavalcanti

NORMALIZAÇÃO BIBLIOGRÁFICA
Coordenadoria de Biblioteca e Pesquisa (Cobip)

Procuradoria-Geral da República
SAF Sul Quadra 4 Conj. C
CEP 70050–900 Brasília - DF
Telefone: (61) 3105–5100
www.mpf.mp.br/pgr

SUMÁRIO

APRESENTAÇÃO

O Programa de Governança em Privacidade (PGP) consiste no conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão do Ministério Público Federal (MPF) quanto à conformidade com a legislação de proteção de dados pessoais.[1]

Mais do que apenas cumprir obrigações legais, o PGP visa demonstrar o compromisso do MPF com a efetivação do direito fundamental à proteção de dados pessoais (art. 5°, LXXIX, da Constituição da República), angariando a confiança de todos os titulares de dados com quem se relaciona: membros, advogados, cidadãos, servidores, colaboradores, contratados, demais partes interessadas e público em geral.

O PGP está previsto no art. 50, §2°, I, da Lei Geral de Proteção de Dados (Lei 13709/2018, LGPD) e no art. 111, I, da Resolução n° 281, de 12 de dezembro de 2023, do Conselho Nacional do Ministério Público (CNMP), que institui a Política Nacional de Proteção de Dados Pessoais e o Sistema Nacional de Proteção de Dados Pessoais no Ministério Público. Esses dispositivos estabelecem os objetivos e requisitos mínimos do PGP:

> "I – 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 a coleta;
>
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados pessoais 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;

---

1 Esse conceito se baseia na definição de "governança pública" estabelecida no Decreto n° 9203/2017, que dispõe sobre a política de governança da administração pública federal. Para melhor compreensão desse conceito, é importante entender também as definições de liderança, estratégia e controle trazidas pelo art. 5° do Decreto:

Art. 5° São mecanismos para o exercício da governança pública:

I - liderança, que compreende conjunto de práticas de natureza humana ou comportamental exercida nos principais cargos das organizações, para assegurar a existência das condições mínimas para o exercício da boa governança, quais sejam:

a) integridade; b) competência; c) responsabilidade; e d) motivação;

II - estratégia, que compreende a definição de diretrizes, objetivos, planos e ações, além de critérios de priorização e alinhamento entre organizações e partes interessadas, para que os serviços e produtos de responsabilidade da organização alcancem o resultado pretendido; e

III - controle, que compreende processos estruturados para mitigar os possíveis riscos com vistas ao alcance dos objetivos institucionais e para garantir a execução ordenada, ética, econômica, eficiente e eficaz das atividades da organização, com preservação da legalidade e da economicidade no dispêndio de recursos públicos.

> f) esteja integrado à 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".

Conforme entendimento da Unidade Especial de Proteção de Dados Pessoais do CNMP (UEPDAP),[2] a expressão "Plano Diretor" é usada na Resolução como equivalente de PGP. Assim, o escopo do PGP pode ser encontrado no art. 35 da Resolução CNMP n° 281/2023, segundo o qual:

> "O Plano Diretor deverá conter as 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, conforme previsto na presente Resolução".

Segundo a Resolução CNMP n° 281/2023, compete ao Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP) de cada ramo e unidade do Ministério Público (art. 50):

> "III - coordenar o processo de elaboração e revisão do Plano Diretor de Proteção de Dados Pessoais;
>
> IV - monitorar a execução do Plano Diretor de Proteção de Dados Pessoais e adotar as providências necessárias à sua implementação e ao seu cumprimento;
>
> V - produzir diagnósticos, estudos e avaliações periódicas a respeito do Plano Diretor de Proteção de Dados Pessoais".

Embora o PGP vise a implantação de uma política de proteção de dados pessoais e alguns de seus artefatos possam ser executados na forma de projetos, ele é um programa permanente, sem previsão de finalização, com uma sucessão de ciclos de melhoria que se perpetuam no tempo.

Para construção deste PGP foi adotado como *framework* o Cronograma da Governança em Privacidade proposto pela UEPDAP/CNMP, que, por sua vez, teve como referência o "Guia de Elaboração de Programa de Governança em Privacidade", de autoria da Secretaria de Governo Digital (SGD)[3].

O Guia da SGD propõe um modelo baseado no Ciclo PDCA (*Plan, Do, Check e Act*), bem como nas normas ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27701:2019 e ABNT NBR ISO/IEC 27005:2011, e está estruturado em 3 etapas, nas quais foram distribuídas as providências necessárias à implantação do PGP (*roadmap*):

2 UEPDAP/CNMP, Coordenação de apoio e orientação aos Ramos e Unidades na implantação da Resolução n° 281 do CNMP. **Orientações para elaboração do Cronograma**, junho de 2024.

3 Secretaria de Governo Digital, **Guia de elaboração de programa de governança em privacidade: Programa de Privacidade e Segurança da Informação (PPSI)**. Brasília: Secretaria de Governo Digital, 2023. 35 p. Versão 2.0. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_programa_governanca_privacidade.pdf. Acesso em: 18 nov. 2024.

INÍCIO

1. Nomeação do Encarregado
2. Alinhamento de Expectativas com a Alta Administração
3. Análise da Maturidade – Diagnóstico do atual estágio de adequação à LGPD
4. Análise e adoção de medidas de segurança, inclusive diretrizes e cultura interna
5. Instituição estrutura organizacional para governança e gestão da proteção de dados pessoais
6. Inventário de Danos Pessoais
7. Levantamento dos contratos relacionados a dados pessoais

8 Políticas e práticas para proteção da privacidade do cidadão

9 Cultura de segurança e proteção de dados e *Privacy by Design*

10 Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

11 Política de Privacidade e Política de Segurança da Informação

12 Adequação de cláusulas contratuais

13 Termo de Uso

14 Indicadores de Performance

15 Gestão de Incidentes

16 Análise de resultados

17 Reporte de resultados

FIM

A UEPDAP/CNMP fez alguns ajustes para adaptar o modelo da SGD às peculiaridades do Ministério Público e contemplar exigências adicionais previstas na Resolução CNMP n° 281/2023. Assim, no cronograma proposto pela UEPDAP foram incluídas a esse *roadmap* as seguintes etapas: na fase de iniciação e planejamento, (a) Tutela Coletiva de Proteção de Dados Pessoais; na fase de construção e execução: (a) Instruções de Serviço; (b) Sistemas informatizados; e (c) Capacitação.

Em setembro de 2024, para atendimento ao disposto no art. 158 da Resolução CNMP n° 281/2023, o MPF entregou à UEPDAP seu cronograma de adequação (anexo ao PGP), construído a partir do modelo proposto. Portanto, a adoção desse mesmo *framework* para elaboração do PGP é a opção mais lógica e natural, pois confere maior racionalidade, eficiência, economia, uniformidade e alinhamento na implementação das ações voltadas à proteção de dados pessoais, além de tornar o PGP um instrumento vivo e operacional.

Nas seções do PGP são abordadas as atividades previstas em cada fase e etapa do programa, contemplando, de forma sucinta e objetiva, o seguinte: (a) descrição das atividades que devem ser implementadas, com referência à fonte normativa, quando cabível; (b) relato das ações que já foram realizadas e o estado atual; (c) explicação do que ainda se pretende fazer e de que maneira.

Em última instância, o objetivo deste programa é que o Ministério Público Federal cumpra sua missão constitucional em consonância com a legislação de proteção de dados pessoais, tanto em suas atividades administrativas como finalísticas. Com isso, espera-se que a instituição continue sendo, ao longo dos próximos anos, uma referência na conformidade e na defesa desse novo direito fundamental.

1 INICIAÇÃO E PLANEJAMENTO

1.1 Nomeação do Encarregado e equipe

De acordo com o art. 44 da Resolução CNMP nº 281/2023, replicando o disposto na LGPD (art. 5º, VIII, e art. 41), o Encarregado é a pessoa indicada pelo controlador e pelo operador para atuar como canal de comunicação entre o controlador, os titulares dos dados pessoais e a Autoridade de Proteção de Dados Pessoais no Ministério Público (APDP/MP), bem como desempenhar outras funções estabelecidas pela legislação pertinente.

No Ministério Público Federal, as atribuições e prerrogativas do Encarregado de Proteção de Dados Pessoais estão descritas nos arts. 96-E e 96-F do Regimento Interno do Gabinete do Procurador-Geral da República (Anexo à Portaria PGR/MPF nº 40, de 24 de abril de 2020), em conformidade com o art. 46 da Resolução CNMP nº 281/2023. O Encarregado deve ser membro da instituição (art. 45 da Resolução CNMP nº 281/2023) e será designado pelo Procurador(a)-Geral da República (art. 96-D do Regimento Interno).

O primeiro Encarregado do MPF foi designado por meio da Portaria PGR/MPF nº 97, de 17 de fevereiro de 2021. O atual Encarregado foi designado pela Portaria PGR/MPF nº 554, de 13 de agosto de 2021 e desempenha suas atribuições por meio de Ofício de Administração (Portaria PGR/MPF nº 521, de 2 de setembro de 2021), de forma cumulada com as atribuições de seu Ofício regular.

Neste ponto, é importante que se acompanhe a evolução da instituição em termos de cultura de proteção de dados pessoais e de maturidade na temática, a fim de antecipar cenários e melhorar a capacidade de tomada de decisão. É possível que os avanços nessas áreas representem, na prática, uma ampliação significativa do volume de demandas e atribuições do Encarregado.

Nesse caso, devem ser empreendidos esforços para que o exercício das funções de Encarregado ocorra, preferencialmente, de forma exclusiva, sem o acúmulo com outras atividades que ensejem o tratamento de dados pessoais. Essa orientação, prevista no art. 45, §1º, da Resolução CNMP nº 281/2023, também contribui para assegurar um cenário de maior autonomia, independência e, principalmente, neutralidade.

O apoio técnico, jurídico e administrativo para o desempenho das atribuições do Encarregado, conforme exigido nos arts. 45, §3º, e 155, parágrafo único, da Resolução CNMP nº 281/2023, é prestado pela Unidade de Proteção de Dados Pessoais (UPDP).

Os dados de contato do Encarregado de Proteção de Dados Pessoais do MPF são públicos e estão acessíveis no Portal do MPF, pelo link: https://www.mpf.mp.br/servicos/lgpd/lgpd-no-mpf/estrutura-da-unidade-de-protecao-de-dados-pessoais.

1.2 Alinhamento de expectativas com a Alta Administração

As primeiras discussões acerca da implementação da LGPD no Ministério Público Federal tiveram início em 2019 por meio de relatório técnico produzido pela Secretaria de Tecnologia da Informação e Comunicação (STIC), nota técnica da Secretaria-Geral (SG) e elaboração da primeira versão do plano de ação, que descrevia as atividades, responsáveis e cronograma para a implementação da LGPD.

A partir de janeiro de 2021, as ações passaram a ser conduzidas pela Comissão de Conformidade à Lei Geral de Proteção de Dados Pessoais do Ministério Público Federal, instituída pela Portaria PGR/MPF nº 24, de 27 de janeiro de 2021 e renovada pela Portaria PGR/MPF nº 580, de 4 de outubro de 2021. A Comissão contou com representantes da Secretaria-Geral, das Secretarias Nacionais, da Ouvidoria e da Consultoria Jurídica do MPF e teve sua atuação coordenada pelo Encarregado de Proteção de Dados Pessoais do MPF (Portaria PGR/MPF nº 97, de 17 de fevereiro de 2021). Seus trabalhos se encerraram em maio de 2022, quando foi criada a Unidade de Proteção de Dados Pessoais (UPDP).

No âmbito interno, o MPF conta, desde 2022, com a Política de Privacidade e Proteção de Dados Pessoais (Portaria PGR/MPF nº 661, de 12 de agosto de 2022). A Política é um marco importante na regulamentação da privacidade e da proteção de dados pessoais nas atividades finalísticas e administrativas institucionais. Ela contempla princípios e diretrizes para tratamento de dados pessoais no MPF, regras sobre contratos, dados sensíveis, dados de crianças e adolescentes e hipóteses de divulgação de dados pessoais, além de disposições sobre agentes de tratamento, segurança da informação e boas práticas.

1.3 Tutela coletiva de proteção de dados

A Resolução CNMP nº 281/2023 estabelece, em seu art. 159, que a tutela coletiva do direito fundamental à proteção de dados pessoais deve ser implantada, de forma imediata, pelos órgãos de execução do Ministério Público.

No Ministério Público Federal, os órgãos de execução que atuam na tutela coletiva do direito fundamental à proteção de dados pessoais, em regra, são os ofícios vinculados à 1ª Câmara de Coordenação e Revisão (Direitos Sociais e Atos Administrativos em geral), presentes em todas as unidades da federação, conforme informa o Ofício GAB/PGR nº 314/2024, encaminhado pelo Vice-Procurador-Geral da República ao CNMP em 09/05/2024.

Além disso, a 3ª Câmara de Coordenação e Revisão (Consumidor e Ordem Econômica) atua na temática da proteção de dados pessoais na área cível, por meio do Grupo de Trabalho de Tecnologia da Informação e Comunicação (GT TIC). Na área criminal, destaca-se o trabalho do Grupo de Atuação Especial no Combate aos Crimes Cibernéticos e aos Crimes praticados mediante o Uso de Tecnologias de Informação no âmbito do MPF, instituído pela Resolução CSMPF nº 229, de 2 de abril de 2024 e vinculado à 2ª Câmara de Coordenação e Revisão.

Embora, nos últimos anos, existam diversas atuações relevantes do MPF na defesa da dimensão coletiva do direito à proteção aos dados pessoais, a evolução almejada pela instituição, em ciclos futuros, deve levar em consideração a necessidade de conscientização e sensibilização contínua da sociedade acerca do tema da proteção de dados pessoais, bem como as diretrizes previstas no parágrafo único do art. 56 da Resolução CNMP nº 281/2023, que apontam para a criação de uma estrutura especializada, com grupos especiais de atuação, capazes de atuar de forma mais proativa e transversal, em caráter nacional, quando necessário.

1.4 Maturidade da instituição

Todos os ramos e as unidades do Ministério Público devem elaborar, anualmente, um relatório de conformidade em relação à Resolução CNMP nº 281/2023. O documento deve seguir os parâmetros estabelecidos na norma e ser enviado à Unidade Especial de Proteção de Dados Pessoais (UEPDAP/CNMP), conforme o art. 161 da Resolução CNMP nº 281/2023.

No Ministério Público Federal, os primeiros diagnósticos de maturidade em proteção de dados pessoais aconteceram antes da vigência da Resolução CNMP nº 281/2023.

Entre novembro de 2020 e maio de 2021, o Ministério Público Federal participou de auditoria realizada pelo TCU para avaliar as ações governamentais e os riscos à proteção de dados pessoais, por meio da elaboração de diagnóstico acerca dos controles implementados pelas organizações públicas federais para adequação à LGPD. O resultado do MPF foi correspondente ao nível "Inicial", valor 0,26, com base em informações prestadas no primeiro trimestre de 2021.

Ainda em 2021, o MPF realizou o diagnóstico de maturidade e índice de adequação à LGPD disponibilizado pelo CNMP, por meio de questionário on-line. O resultado posicionou a instituição no nível básico (índice 0,3, em escala de 0 a 1), à frente de outros ramos do MPU, mas ainda distante da plena adequação à LGPD. Em 2022, a UPDP realizou novo diagnóstico de maturidade e índice de adequação à LGPD disponibilizado pelo CNMP. O MPF foi posicionado no nível intermediário (índice 0,57, em escala de 0 a 1).

Em dezembro de 2022, a UPDP elaborou, com base na matriz de diagnóstico do TCU, novo diagnóstico de maturidade e índice de adequação à LGPD. O resultado da aferição posicionou o MPF no nível intermediário (índice 0,76, em escala de 0 a 1).

Em 2023, a UPDP elaborou diagnóstico de conformidade à Resolução CNMP nº 281/2023, com base no modelo de relatório de conformidade anexado à norma (em forma de questionário). O resultado revelou que 80% das medidas foram implementadas (62% integralmente e 18% parcialmente). Apenas 20% dos itens ainda não tinham sido atendidos.

Ainda em 2023, o MPF realizou o diagnóstico do Programa de Privacidade e Segurança da Informação (PPSI), da Secretaria de Governo Digital, que estabelece, além do índice relativo à cibersegurança, o índice de privacidade (iPriv), com 150 questões distribuídas em 13 dimensões. Em relação ao Índice de Privacidade do PPSI (iPriv), o MPF alcançou o valor de 0,70, em escala de 0 a 1. Esse valor corresponde, segundo aquele programa, ao nível "Em aprimoramento", apenas um nível abaixo da pontuação máxima.

Em 2024, a Unidade de Proteção de Dados Pessoais encaminhou à UEPDAP/CNMP o primeiro relatório de conformidade, nos termos do art. 161 da Resolução CNMP nº 281/2023. O resultado revelou que 90,9% das medidas foram implementadas, sendo que 65,9% estão integralmente implementadas e 25% estão parcialmente implementadas. Apenas 9,1% dos requisitos ainda não foram atendidos.

Recentemente, o MPF passou por nova auditoria do TCU e aguarda o resultado do diagnóstico. Além disso, o MPF pretende realizar, anualmente, dois diagnósticos de maturidade em privacidade e proteção de dados pessoais: um nos moldes definidos pela UEPDAP/CNMP e outro seguindo os parâmetros de privacidade do Programa de Privacidade e Segurança da Informação (*Framework* da Secretaria de Governo Digital).

1.5 Medidas de segurança

A LGPD estabelece que o tratamento de dados pessoais deve ser revestido das melhores práticas de segurança da informação. De acordo com o art. 46 da LGPD, tanto o controlador como o operador 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.

O art. 47 exige que as medidas de segurança acompanhem todo o ciclo de vida do dado, devendo ser garantidas mesmo após o término do tratamento.

O MPF conta, atualmente, com equipe dedicada à gestão, defesa e monitoramento de segurança cibernética, bem como à continuidade e recuperação de serviços de TI.

Além disso, segundo os arts. 124 e 125 da Resolução CNMP nº 281/2023, o Ministério Público deve determinar que todos os seus integrantes - membros, servidores, estagiários e prestadores de serviço - assinem Termo de Compromisso de Manutenção de Sigilo (TCMS), bem como as partes a fim de assegurar a proteção dos dados pessoais tratados na instituição.

O Ministério Público Federal já adota a prática de assinatura de TCMS quando do ingresso de membros e servidores, na contratação de estagiários e na celebração de contratos que envolvem prestadores de serviços. A recomendação para o próximo ciclo é a adoção do modelo de TCMS elaborado pela UEPDAP/CNMP.

1.6 Estrutura organizacional para a governança e gestão da proteção de dados pessoais

Para realizar a governança e a gestão da temática proteção de dados pessoais, o Ministério Público Federal atualmente conta com o Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP), instituído pela Portaria PGR/MPF nº 64, de 26 de janeiro de 2024 e com a Unidade de Proteção de Dados Pessoais (UPDP), cuja estrutura foi estabelecida pela Portaria PGR/MPF nº 366, de 18 de maio de 2022 e as competências e atribuições foram definidas na Portaria PGR/MPF nº 795, de 26 de setembro de 2022.

O CEPDAP é um órgão colegiado de caráter permanente. Sua criação, composição e atribuições foram determinadas nos art. 49 a 55 da Resolução CNMP nº 281/2023. O comitê é presidido pelo Encarregado de Proteção de Dados Pessoais e é composto por representantes da Corregedoria-Geral, Ouvidoria, Secretaria Geral, Secretaria de Segurança Institucional, Secretaria de Tecnologia da Informação e Comunicação, Secretaria de Gestão de Pessoas e Secretaria Jurídica e de Documentação. Dentre as competências destacam-se a de propor mecanismos e instrumentos para a investigação e a prevenção de quebra de segurança da informação relativa a dados pessoais, bem como para o tratamento da informação sigilosa comprometida concernente a dados pessoais, além de sugerir critérios acerca da publicidade dos atos quando envolverem a exibição de dados pessoais mantidos pela instituição.

Por sua vez, a Unidade de Proteção de Dados Pessoais (UPDP) constitui a estrutura administrativa que presta ao Encarregado de Proteção de Dados Pessoais e ao CEPDAP apoio técnico, jurídico e administrativo para o desempenho de suas atribuições, conforme previsto nos arts. 45, §3º, e 155, parágrafo único, da Resolução CNMP nº 281/2023.

A Unidade é subordinada diretamente ao Procurador-Geral da República e tem sua estrutura e atribuições previstas no Regimento Interno do Gabinete do Procurador(a)-Geral da República (arts. 96-G a 96-L), competindo-lhe, de modo geral, o planejamento, coordenação, monitoramento e controle das ações de conformidade com a LGPD. A estrutura atual da UPDP compreende a Secretaria Executiva, Assessoria Administrativa e Assessoria Técnica. No futuro, está planejada uma reestruturação da UPDP para fins de adequação à Resolução CNMP nº 281/2023 e criação de uma nova assessoria cujas atribuições estão relacionadas à governança, conformidade documental e monitoramento.

1.7 Inventário de dados pessoais

O registro das operações de tratamento de dados pessoais (ROT), previsto no art. 37 da LGPD como obrigação do controlador de dados, consiste na identificação, documentação e visualização do fluxo real de dados pessoais dentro da organização. O ROT deve conter informações sobre como os dados são coletados, processados, armazenados e compartilhados.

O ROT de dados pessoais é realizado para cada um dos processos de trabalho da organização, conforme previsto no art. 80, §1° da Resolução CNMP 281/2023 e a recomendação do Guia de Inventário de Dados Pessoais da Secretaria de Governo Digital.

Em 2021, foi iniciado o levantamento para a criação do registro das operações de tratamento (ROT) dos dados pessoais pela Comissão de Conformidade à LGPD do MPF. Naquele momento, os gestores das áreas administrativas responderam ao questionário acerca dos processos de trabalhos que envolviam tratamento de dados pessoais. Após, os dados foram validados pela UPDP em conjunto com o Encarregado de Proteção de Dados Pessoais.

Atualmente, os dados estão registrados em sistema desenvolvido para consolidação das informações (LGPD Processos) e encontram-se em validação pelos gestores de cada processo de trabalho, com conclusão prevista para o primeiro trimestre de 2025. No ciclo seguinte está prevista a ampliação das atividades, com o mapeamento dos processos de trabalho voltados para a área finalística da instituição. Também se pretende a contratação de uma ferramenta abrangente de governança de dados para garantir o tratamento seguro e dar ampla visibilidade aos dados, a fim de mitigar riscos à segurança e à privacidade.

1.8 Levantamento dos contratos relacionados a dados pessoais

Todo contrato realizado no âmbito da Administração Pública envolve, em alguma medida, o tratamento de dados pessoais, seja, exclusivamente, para cumprir a exigência legal de qualificação das partes e de seus representantes (art. 89, § 1°, da Lei 14133/2021), seja para cumprir também o seu objeto.

O MPF relacionou todos os contratos vigentes celebrados com instituições públicas e privadas e analisou o nível de proteção de dados pessoais presente nesses instrumentos, especialmente quanto à sua compatibilidade com os elementos de risco envolvidos nas operações de tratamento de dados pessoais identificadas e com o papel exercido pelas partes enquanto agentes de tratamento.

A fim de possibilitar a análise e a categorização dos contratos quanto ao nível de proteção de dados pessoais, foram feitos ajustes no Sistema de Gestão Administrativa - SGA, como a inclusão de campos para identificar a existência de tratamento de dados pessoais e de cláusulas de proteção e dados pessoais.

Esse levantamento será utilizado para orientar tanto as ações de adequação de contratos vigentes aos princípios e regras de proteção de dados pessoais previstos na Resolução CNMP n° 281/2023 e na LGPD, quanto a elaboração de modelos de cláusulas de proteção de dados pessoais para novas contratações.

2 CONSTRUÇÃO E EXECUÇÃO

2.1 Políticas e práticas para proteção da privacidade do cidadão

Como boa prática em relação à proteção de dados pessoais (art. 50, LGPD), o MPF publica diversas informações sobre as atividades desenvolvidas pelo encarregado e pela equipe dedicada à temática no Portal do MPF.

Além disso, em atendimento ao art. 166 da Resolução CNMP nº 281/2023, são promovidas regularmente campanhas de comunicação, veiculadas nos canais internos, com o objetivo de fomentar uma cultura de proteção de dados pessoais na instituição.

Nas três últimas edições, o foco das campanhas foi o de esclarecer questões conceituais acerca da LGPD, informar ao público interno sobre os direitos e garantias oferecidos pela Lei, orientar sobre cuidados a serem adotados, individualmente, para proteger os dados pessoais próprios e o de terceiros e orientar sobre a correta aplicação da Lei Geral de Proteção de Dados na atividade finalística. A próxima campanha de comunicação será direcionada ao público externo com a finalidade de ampliar o alcance, disseminar o conhecimento, sensibilizar a sociedade acerca da importância da defesa desse direito fundamental e do papel do Ministério Público.

2.2 Cultura de segurança e proteção de dados e privacidade desde a concepção (*privacy by-design*)

A privacidade desde a concepção consiste em assegurar a privacidade do titular dos dados pessoais desde o início e durante todo o ciclo de vida de um projeto, sistema, serviço, produto ou processo de trabalho. Ao abordar essa temática, a LGPD estabelece que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de tratamentos inadequados ou ilícitos, desde a coleta até sua eliminação (art. 46).

• A fim de consolidar a cultura de segurança e proteção de dados e privacidade desde a concepção, a STIC publicou, em novembro de 2022, a Orientação Técnica nº 17 - Privacidade desde o projeto. O documento contém diretrizes para que a privacidade seja levada em consideração em todas as etapas de desenvolvimento dos produtos no MPF, sejam eles *softwares*, *hardwares*, serviços, processos de trabalho, práticas, tecnologias ou infraestrutura.

• Estão previstos, para 2025, o *checklist* de privacidade, voltado ao desenvolvimento de produtos e serviços que envolvem o tratamento de dados pessoais, e a certificação de conformidade Privacidade desde a Concepção, que consiste no reconhecimento, por meio de selo de conformidade, da aderência aos princípios e controles do *Privacy by Design*.

2.3 Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

O Relatório de Impacto à Proteção Dados Pessoais - RIPD, previsto nos arts. 137 a 144 da Resolução CNMP nº 281/2023 e no parágrafo único do art. 38 da LGPD, visa avaliar os riscos do tratamento de dados pessoais. No RIPD devem ser identificados os tipos de dados pessoais, as categorias de titulares, o fluxo dos dados pessoais, os riscos, as medidas e controles a serem adotados.

Trata-se de um processo concebido para descrever o tratamento e auxiliar na gestão dos riscos que possam impactar nos direitos e liberdades dos titulares de dados. Esses impactos são

avaliados e documentados, de modo que medidas adequadas sejam tomadas para prevenir, mitigar ou até mesmo aceitar riscos que possam gerar impactos negativos.

Antes do advento da Resolução CNMP nº 281/2023, o MPF elaborou um documento com diretrizes para orientar a elaboração do RIPD. No próximo ciclo, o documento será submetido à adequação, de acordo com as orientações da UEPDAP/CNMP, e serão selecionados os sistemas, bases de dados e processos de trabalho para elaboração do RIPD.

2.4 Medidas e Política de Segurança da Informação e Política de Proteção de Dados Pessoais

A Política Nacional de Cibersegurança do Ministério Público, instituída pela Resolução CNMP nº 294, de 28 de maio de 2024, dispõe sobre as medidas voltadas à segurança da informação nos meios de tecnologia da informação e comunicação. Muitas dessas medidas, como estrutura de gerenciamento da segurança da informação e privacidade, controle de acesso aos dados pessoais, registros de eventos, criptografia e adoção da privacidade desde a concepção, dialogam com a proteção de dados pessoais.

Atualmente, o MPF adota, como boa prática, o *framework* do Programa de Privacidade e Segurança da Informação (PPSI). O Programa envolve um conjunto de ações de adequação na temática, voltadas para melhoria no grau de maturidade e de resiliência das instituições, e estabelece índice relativo à cibersegurança e índice de privacidade, baseado nos controles do *Center for Internet Security* (CIS) - conjunto de práticas que visam proteger organizações contra as ameaças cibernéticas mais comuns e perigosas.

Entre as diversas medidas de segurança da informação implementadas pelo MPF, relacionadas à proteção de dados pessoais, destacam-se o duplo fator de autenticação provido pelo Google e a autenticação via ferramenta do Governo Federal, o Gov.br; o monitoramento e a revogação de acesso e de disponibilização de sistemas para o público interno, por meio de autenticação em portal (Instrução Normativa SG/MPF nº 38, de 21 de novembro de 2023); e o registro em logs para auditoria e aplicação de política de backup e restauração de sistemas e serviços (Instrução Normativa SG/MPF nº 3, de 6 de março de 2023).

O MPF também vem trabalhando no desenvolvimento de ferramenta que faz uso de inteligência artificial para a pseudonimização automatizada de dados pessoais em documentos. Também está em curso a implementação da tabela de temporalidade, a fim de indicar o momento de eliminação dos dados pessoais, quando cumprida a sua finalidade.

No próximo ciclo, vislumbra-se a disponibilização da ferramenta de pseudonimização para uso na instituição no primeiro semestre de 2025. Em relação à eliminação dos dados pessoais, pretende-se evoluir para a definição de fluxos de trabalho e implantação de regras nos sistemas.

A Política de Segurança da Informação do MPF está em fase de desenvolvimento, em conformidade com a LGPD e a Resolução nº 281/2023. Os demais normativos que versam sobre o mesmo tema passarão por adequações à legislação de proteção de dados pessoais.

2.5 Adequação de cláusulas contratuais

A instrumentalização das regras de proteção de dados pessoais em contratos do MPF pode ser feita por meio de cláusulas de proteção de dados pessoais, quando o contrato ainda está em fase

de elaboração, ou por meio de aditivo que insira cláusulas de proteção de dados pessoais, nos casos em que o contrato tenha sido firmado.

A Resolução CNMP nº 281/2023, em seu art. 171, estabelece que todos os contratos e convênios em vigor que envolvem o tratamento de dados pessoais devem ser adequados a seus padrões. Essa orientação se aplica a todos os tipos de instrumentos contratuais.

A fim de cumprir o disposto na legislação de proteção de dados pessoais, o MPF realizou ajustes em sistemas, mapeou e classificou os contratos, de acordo com a criticidade, identificou os contratos de tecnologia, para fins de priorização de adequação, e elaborou cláusulas-modelo de proteção de dados pessoais, para serem utilizadas em termos aditivos e em novas contratações.

Concluído esse levantamento, as áreas responsáveis foram acionadas para dar início ao processo de adequação dos instrumentos contratuais. O trabalho de adequação/inserção das referidas cláusulas foi iniciado em todas as unidades do MPF. Para auxiliar nesse trabalho, foi elaborada uma cartilha sobre proteção de dados pessoais em contratos. O monitoramento e auditoria dessas adequações estão previstos para o próximo ciclo.

2.6 Termos de uso e Política de Privacidade

A LGPD assegura ao titular o direito de acesso facilitado às informações sobre o tratamento de seus dados (art. 9º) e estabelece que o Poder Público deve informar as hipóteses em que, no exercício de suas competências, realiza o tratamento de dados pessoais (art. 23, I). Esse conjunto de informações é chamado de Aviso de Privacidade, de acordo com a norma ABNT NBR ISO/IEC 29184:2021.

Todo serviço ou produto que envolve o tratamento de dados pessoais, on-line ou não, deve conter um aviso de privacidade em sua página inicial, em formulários on-line, em aplicativos móveis e nos demais canais disponíveis ao usuário. Pode até mesmo ser fixado em quadros de aviso impresso. Ele deve ser redigido de forma concisa, acessível e com uso de linguagem simples e clara, paralelamente à elaboração do mapeamento do respectivo processo. Pode ser apresentado em camadas e com a utilização de elementos visuais, assegurando a acessibilidade aos cegos.

Além disso, é necessário que exista um ambiente que reúna todos os avisos de privacidade, com links e imagens, para que o titular de dados pessoais consiga localizar, com facilidade, as informações de seu interesse. Publicados no Portal do MPF, eles reúnem informações gerais sobre os serviços/sistemas ofertados pela instituição e contam ainda com os Avisos de Privacidade específicos, incluindo Política de Cookies, todos elaborados em linguagem simples e acessível, voltados ao público externo e interno. Sempre que necessário, os avisos devem ser atualizados, preservando as versões anteriores pelo mesmo período em que forem mantidos os dados associados ao serviço.

Para o próximo ciclo, almeja-se garantir a conformidade legal nesse processo de adequação contínua dos normativos e reestruturação dos avisos de privacidade para fins de simplificação e acesso fácil às informações.

Além dos Avisos de Privacidade, está disponível no portal do MPF a Política de Privacidade e Proteção de Dados Pessoais no MPF, conforme estabelecido no art 132, III e VI, da Resolução CNMP nº 281/2023. Ela foi instituída em agosto de 2022, por meio da Portaria PGR/MPF nº 661, e regulamentou a proteção de dados pessoais nas atividades finalísticas e administrativas do Ministério Público Federal, bem como no relacionamento do órgão com membros,

advogados, cidadãos, servidores, colaboradores, contratados, demais partes interessadas e público em geral.

2.7 Instruções de serviço

De acordo Resolução CNMP nº 281/2023, todos os ramos e unidades do Ministério Público, na qualidade de controladores e órgãos gestores locais do Sistema Nacional de Proteção de Dados Pessoais do MP, devem normatizar e deliberar a respeito das regras de tratamento de dados pessoais no âmbito da instituição, bem como expedir instruções de serviço quanto às normas de segurança, padrões técnicos e obrigações específicas para os envolvidos no tratamento dos dados pessoais (art. 38, I).

O Ministério Público Federal relacionou os atos normativos que necessitam de adequação à legislação de proteção de dados pessoais e elaborou cronograma para a realização desse trabalho, iniciado a partir das instruções normativas da instituição, nos termos previstos no art. 156 da Resolução CNMP nº 281/2023. A execução do cronograma será acompanhada pela UPDP, que prestará apoio na elaboração dos dispositivos de proteção de dados pessoais a serem inseridos nos normativos.

O quadro a seguir relaciona os atos normativos identificados, afetos à temática da proteção de dados, objeto de análise, revisão (se necessário) e monitoramento, para fins de conformidade à legislação. Essa relação é passível de atualização a qualquer tempo.

TEMA	ATO NORMATIVO
SEGURANÇA DE DADOS	**BACKUP DE ARQUIVOS:** **Instrução Normativa SG/MPF nº 3, de 6 de março de 2023 -** Dispõe sobre a institucionalização da política de cópia de segurança (Backup) e restauração de arquivos digitais no âmbito do Ministério Público Federal. Íntegra.
	SEGURANÇA DA INFORMAÇÃO: **Portaria PGR/MPF nº 417, de 5 de julho de 2013 -** Dispõe sobre o Plano de Segurança Institucional do Ministério Público Federal. Íntegra. **Portaria PGR/MPF nº 980, de 12 de novembro de 2018** - Dispõe sobre a Política de Segurança Institucional do Ministério Público Federal. Íntegra.
	POLÍTICA DE SENHAS: **Instrução Normativa SG/MPF nº 11, de 7 de agosto de 2014 -** Dispõe sobre os critérios mínimos de segurança de senhas de contas de usuários, de equipamentos e de aplicações no âmbito do Ministério Público Federal. Íntegra.
	EMISSÃO DE CERTIFICADOS DIGITAIS: **Instrução Normativa SG/MPF nº 5, de 10 de junho de 2022 -** Dispõe sobre o processo de emissão de certificados digitais para os membros, servidores, equipamentos e aplicações do Ministério Público Federal. Íntegra.
DIVULGAÇÃO E COMPARTILHAMENTO DE DADOS	**VIDEOCONFERÊNCIA, TRANSMISSÃO E GRAVAÇÃO DE EVENTOS NO MPF** **Instrução Normativa SG/MPF nº 12, de 11 de abril de 2023 -** Dispõe sobre a utilização de serviços de videoconferência e os procedimentos de transmissão e gravação de eventos no âmbito do Ministério Público Federal. Íntegra.

TEMA	ATO NORMATIVO
	TVMPF **Instrução Normativa SG/MPF nº 16, de 13 de setembro de 2019 -** Regulamenta a utilização do Portal de Vídeos Institucionais, denominado TV MPF, no âmbito do Ministério Público Federal. Íntegra.
	MPF DRIVE **Instrução Normativa SG/MPF nº 13, de 10 de novembro de 2020 -** Dispõe sobre a política de uso do serviço de acesso, compartilhamento e edição de arquivos em nuvem do Ministério Público Federal, MPF Drive. Íntegra.
	CORREIO ELETRÔNICO **Portaria PGR/MPF nº 425, de 5 de julho de 2013 -** Dispõe sobre os procedimentos de centralização dos serviços de correio eletrônico no âmbito do Ministério Público Federal. Íntegra.
IDENTIFICAÇÃO DE DADOS PESSOAIS	**Portaria SG/MPU nº 21, de 28 de julho de 2021 -** Disponibiliza tabela específica contendo os documentos que compõem os assentamentos funcionais dos servidores do Ministério Público da União. Íntegra.
ARMAZENAMENTO/ ELIMINAÇÃO/ GUARDA	**Portaria PGR/MPF nº 101, de 24 de fevereiro de 2021 -** Estabelece os parâmetros para os processos de recolhimento, organização, descrição, difusão e preservação de documentos arquivísticos permanentes do Ministério Público Federal. Íntegra.
	Instrução Normativa SG/MPF nº 11, de 26 de setembro de 2018 - Estabelece processo para eliminação de documentos arquivísticos do Ministério Público Federal. Íntegra.
	Portaria PGR/MPF nº 184, de 21 de março de 2016 - Aprova os instrumentos arquivísticos de gestão documental da área fim do Ministério Público Federal e dá outras providências. Íntegra.
	Instrução Normativa SG/MPF nº 3, de 30 de dezembro de 2002 - Estabelece normas e procedimentos para o arquivamento de processos e documentos administrativos. Íntegra.
	Portaria SG/MPF nº 858, de 30 de dezembro de 2002 - Publica a atualização da Tabela de Temporalidade de Documentos do Ministério Público Federal. Íntegra.
	Instrução Normativa SG/MPF nº 4, de 27 de abril de 2021 - Estabelece o processo de recolhimento de documentos arquivísticos físicos do Ministério Público Federal. Íntegra.
	Instrução Normativa SG/MPF nº 20, de 11 de julho de 2023 - Dispõe sobre a utilização da solução contratada de correio eletrônico em nuvem no âmbito do Ministério Público Federal. Íntegra.
CLASSIFICAÇÃO DA INFORMAÇÃO	**Portaria PGR/MPF nº 204, de 23 de abril de 2013 -** Estabelece os procedimentos a fim de assegurar o direito de acesso à informação no âmbito do Ministério Público Federal. Íntegra.
	Portaria SG/MPF nº 454, de 29 de junho de 2018 - Estabelece procedimentos de restrição de acesso a informações pessoais de membros e servidores quanto ao seu tratamento, proteção, acesso, transmissão e divulgação no âmbito do Ministério Público Federal. Íntegra.

TEMA	ATO NORMATIVO
	Portaria PGR/MPF nº 590, de 24 de setembro de 2021 – Dispõe sobre o sistema Único. Íntegra.
ACESSO À INFORMAÇÃO	**Portaria PGR/MPF nº 480, de 1º de outubro de 2009 -** Dispõe sobre a divulgação de dados e informações de gestão da Administração do MPF, por meio da Rede Mundial de Computadores - Internet, e institui a Comissão Reguladora do Portal da Transparência do Ministério Público Federal. Íntegra.
	Portaria PGR/MPF nº 204, de 23 de abril de 2013 - Estabelece os procedimentos a fim de assegurar o direito de acesso à informação no âmbito do Ministério Público Federal. Íntegra.
	Portaria PGR/MPF nº 412, de 5 de julho de 2013 - Institui a Sala de Atendimento ao Cidadão no âmbito do Ministério Público Federal. Íntegra.
COLETA DE DADOS	**Portaria PGR/MPF nº 12, de 22 de janeiro de 2013 -** Dispõe sobre o Sistema de Controle de Acesso às instalações da Procuradoria Geral da República e dá outras providências. Íntegra.
	Portaria PGR/MPF nº 1.213, de 26 de dezembro de 2018 - Dispõe sobre o recebimento e a gestão de documentos protocolados junto ao Ministério Público Federal. Íntegra.
CONDUTA ÉTICA	**Portaria PGR/MPU nº 98, de 12 de setembro de 2017 -** Aprova o Código de Ética e de Conduta do Ministério Público da União e da Escola Superior do Ministério Público da União. Íntegra.
	Portaria SG/MPF nº 721, de 15 de dezembro de 2021 - Institui o Código de Conduta, Integridade e Compliance do Plan-Assiste do Ministério Público da União. Íntegra.
GESTÃO DE RISCOS	**Portaria PGR/MPU nº 78, de 8 de agosto de 2017 -** Institui a Política de Gestão de Riscos do Ministério Público da União. Íntegra.
	Portaria PGR/MPF nº 155, de 24 de março de 2022 - Dispõe sobre a Gestão de Riscos no Ministério Público Federal e aprova o Plano de Gestão de Riscos do Ministério Público Federal. Íntegra.
SAÚDE	**Portaria PGR/MPF nº 638, de 17 de agosto de 2023 -** Regulamenta a avaliação pericial administrativa em saúde, os atestados médicos e odontológicos e a concessão de licenças aos servidores do Ministério Público Federal. Íntegra.
	Ato Conjunto PGR/PGT/PGJM/PGJDFT nº 2, de 30 de setembro de 2022 - Aprova a unificação das estruturas administrativas do Plan-Assiste no âmbito do Ministério Público da União e dá outras providências. Íntegra.
	Ato Conjunto PGR/PGT/PGJM/PGJDFT nº 5, de 20 de dezembro de 2022 - Complementa o Ato Conjunto PGR/PGT/PGJM/PGJDFT nº 2, de 30 de setembro de 2022, estabelecendo as diretrizes e parâmetros a serem adotados para a unificação do Plan-Assiste, bem como, os direitos e obrigações de cada ramo do MPU, e dá outras providências. Íntegra.
	Ato Conjunto PGR/PGT/PGJM/PGJDFT nº 5, de 9 de agosto de 2023 - Complementa o Ato Conjunto PGR/PGT/PGJM/PGJDFT nº 5, de 20 de dezembro de 2022, para estabelecer a estrutura organizacional, de pessoal e de cargos em comissão e funções de confiança do Plan-Assiste/MPU nos estados. Íntegra.

2.8 Sistemas informatizados

Ainda que o tratamento de dados pessoais nos procedimentos, serviços, sistemas, portais, aplicativos e plataformas do Ministério Público Federal seja regulamentado por atos normativos específicos, com o objetivo de atender suas particularidades, eles devem ser publicados e interpretados segundo os princípios e diretrizes (art. 2°, § 1) da Política de Privacidade e Proteção de Dados Pessoais no MPF (Portaria PGR/MPF n° 661, de 12 de agosto de 2022).

Os sistemas informatizados do MPF já contam com a adoção de medidas de segurança como: controle de acesso, política de backup, log de auditoria, manter bases de produção e não produção separadas. Porém, há a necessidade de implementar de forma global algumas medidas atualmente adotadas em alguns sistemas, como é o caso do múltiplo fator de autenticação e a varredura de antivírus em arquivos.

2.9 Capacitação

Devem ser ofertadas, de forma contínua, ações de capacitação para disseminar conhecimento, sensibilizar e promover a cultura de proteção dos dados pessoais, junto a membros, servidores e colaboradores no Ministério Público Federal (art. 1, II e art. 47, §6°, Resolução CNMP n° 281/2023 e art. 22 da Política de Privacidade e Proteção de Dados Pessoais no MPF).

Boas práticas de proteção de dados pessoais são disponibilizadas por meio de cursos, com instrutoria interna ou externa, preferencialmente na modalidade online, sobre: a proteção de dados pessoais, a privacidade como direito fundamental, acesso à informação, segurança da informação, avaliação de riscos, governança de dados, normas da família ISO, entre outros.

Os treinamentos e capacitações são oferecidos por níveis: do mais básico ao mais complexo, incluindo certificações profissionais no tema e afins. Além de constar do plano de capacitação da SGP, deverá ser disponibilizada na página da UPDP uma relação de cursos, gratuitos ou não, sobre a temática. Sempre que o orçamento permitir e a situação assim necessitar, serão realizados, anualmente, eventos sobre o tema, especialmente nas semanas do dia internacional da proteção de dados (28/01), do dia nacional da proteção de dados pessoais (17/07) e do aniversário da LGPD (14/08), de modo a contribuir com a formação e manutenção da cultura de privacidade institucional.

3 MONITORAMENTO

As práticas previstas neste programa devem ser periodicamente monitoradas para verificar se os objetivos estão sendo atingidos, se os recursos estão sendo empregados de forma racional, se as entregas estão sendo maximizadas em relação aos recursos empregados e se os resultados estão indo em direção à conformidade com a legislação de proteção de dados pessoais.

O monitoramento, cíclico e contínuo, permitirá a tomada de decisão baseada em dados, a correção de eventuais desvios, a identificação de oportunidades de melhorias e a promoção do aprendizado constante, com o intuito de orientar as ações da gestão que, por sua vez, também fornecerá insumos para avaliação e ajustes deste programa.

Dessa forma, será preciso estabelecer as rotinas para o levantamento das informações necessárias ao monitoramento, implantar os indicadores de desempenho, monitorar a execução do plano de ação quanto aos prazos e metas e definir o formato e a periodicidade dos relatórios de gestão.

3.1 Indicadores de performance

Os indicadores de performance visam medir o nível de sucesso da execução do programa e se suas entregas estão de acordo com os objetivos a serem alcançados. Os indicadores deverão mensurar a execução e o resultado das práticas, no decurso de um ano. Além de demonstrar o estado de implementação do PGP, os resultados apurados permitirão realizar correções no rumo e, assim, evitar retrabalhos no futuro.

INDICADOR	DESCRIÇÃO	PERIODICIDADE	FONTE	META
IND01 - Conscientização	Quantidade de ações de treinamento e campanhas realizadas no período / Quantidade de ações de treinamento e campanhas previstas no período X 100	Anual	Intranet, EAD, Plano de ação da UPDP, Proposta de cursos, Plano de Comunicação	50% ⬆
ND02 – Operações de tratamento registradas	Quantidade de processos de trabalho que tratam dados pessoais registrados e revisados / Quantidade de processos de trabalho que tratam dados pessoais (área administrativa) X 100	Anual	Intranet, EAD, Plano de ação da UPDP	80% ⬆
IND03 - Avisos de Privacidade	Quantidade de serviços com aviso de privacidade elaborado / Quantidade de serviços oferecidos pela instituição que tratam dados pessoais X 100	Anual	Portal do MPF; Reuniões com gestores; Formulário Aviso de Privacidade	80% ⬆
IND04 - Atendimento aos titulares de dados	Quantidade de demandas de titulares de dados atendidas fora do prazo / Quantidade de demandas de titulares recebidas X 100	Anual	LGPD Consulta, Correio eletrônico UPDP e Sistema Único	10% ⬇
IND05 - Adequação de contratos	Número de contratos revisados com inclusão de cláusulas de conformidade à LGPD / quantidade de contratos que precisam de revisão X 100	Anual	SGA	80% ⬆

INDICADOR	DESCRIÇÃO	PERIODICIDADE	FONTE	META
IND06 - Avaliação de Impacto à Proteção de Dados	Quantidade de processos com RIPD elaborados / Quantidade de processos da instituição que necessitam de RIPD X 100	Anual	LGPD Processos	50% ↑

3.2 Gestão de incidentes

A LGPD prevê que os controladores e operadores deverão contar com planos de resposta a incidentes e remediação (art. 50, §2°, I, "g"). Por sua vez, a Política de Privacidade e Proteção de Dados Pessoais no MPF (Portaria PGR/MPF n° 661, de 12 de agosto de 2022) prevê a instituição do Plano de Resposta a Incidentes de Segurança com Dados Pessoais (art. 21, parágrafo único).

Desde junho de 2023, o MPF possui um Plano de Resposta a Incidentes de Segurança com Dados Pessoais (PRISDP), formalizado por meio da Orientação Técnica n° 18 da STIC. O PRISDP dispõe sobre a abrangência do plano, os atores e suas responsabilidades, as diretrizes de notificação e os procedimentos internos e externos frente a incidentes de segurança, com o objetivo de propiciar uma resposta ágil e efetiva a incidentes com dados pessoais, reduzindo ao máximo os impactos aos direitos e liberdades dos titulares de dados.

O processo de resposta a incidentes de segurança com dados pessoais está mapeado e integra a arquitetura de processos do MPF (PS.03.05.03). Em síntese, ele contempla as seguintes etapas:

1. **Preparação:** (a) formação da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR); (b) instalação e divulgação dos mecanismos de comunicação de incidentes; (c) mapeamento de ativos de informação, de gestão de riscos de segurança da informação, de gestão de continuidade de negócios em segurança da informação e de gestão de mudanças nos aspectos de segurança da informação; (d) implementação de controles de segurança, de gerenciamento de vulnerabilidades, de conscientização e de capacitação.

2. **Detecção e análise do incidente:** (a) triagem, priorização e classificação; (b) análise; (c) notificações ao encarregado e, conforme avaliação de relevância do incidente, às autoridades de proteção de dados e titulares dos dados violados.

3. **Tratamento e resposta:** (a) contenção; (b) coleta de evidências; (c) erradicação; (d) recuperação.

4. **Atividades pós-incidentes:** (a) lições aprendidas; (b) uso dos dados coletados; (c) retenção de evidências.

Além do monitoramento diário realizado pela área técnica e de segurança, o PRISDP prevê canais pelos quais qualquer pessoa, interna ou externa, pode comunicar um incidente de segurança de que suspeite ou tenha conhecimento. Internamente, o canal a ser utilizado é o SNP (Sistema Nacional de Pedidos), pelo serviço: Segurança da Informação – Incidente da Segurança da Informação. Externamente, o canal a ser utilizado é o de e-mail através das caixas abuse@mpf.mp.br ou csirt@mpf.mp.br, informados no Portal do MPF Serviços.

Com o advento da Resolução CNMP n° 281/2023, o PRISDP precisará passar por revisão para adequação à norma (art. 145 a 152), especialmente quanto aos critérios para avaliação da rele-

vância do incidente e a substituição da ANPD pela UEPDAP/CNMP como autoridade à qual devem ser dirigidas as comunicações de incidentes de segurança com dados pessoais.

3.3 Análise de resultados

Caberá à Unidade de Proteção de Dados Pessoais, com periodicidade anual, a análise das ações realizadas em cumprimento a este PGP e a elaboração do relatório de atividades desenvolvidas durante o ano, a fim de identificar os resultados alcançados, apontar as dificuldades e principais desafios encontrados, bem como propor soluções e ajustes ao programa para deliberação do CEPDAP.

3.4 Reporte de resultados

O relatório anual deve ser apresentado ao CEPDAP e, após aprovação, ser enviado ao Procurador-Geral da República, bem como disponibilizado no portal do MPF na internet para consulta do público em geral. O relatório, na medida do possível, deve espelhar a estrutura do PGP, com linguagem clara e simples e o uso de recursos visuais.

4 CRONOGRAMA DE IMPLANTAÇÃO

DESCRIÇÃO		DIAS	INÍCIO	TÉRMINO
1	**Iniciação e Planejamento**			
1.1	**Nomeação do Encarregado e Equipe**			
1.1.1	Constituir o Encarregado (arts. 34 e 47)	90	Ter 27/02/24	Ter 27/02/24
1.1.2	Constituir o Comitê Estratégico de Proteção de Dados (arts. 34 e 49)	90	Ter 27/02/24	Ter 27/02/24
1.1.3	Publicar no site o nome e qualificação do Encarregado (artigo 65, parágrafo único)	180	Ter 27/02/24	Ter 27/02/24
1.2	**Alinhamento de Expectativas com a Alta Administração**			
1.2.1	Reunião do Comitê Estratégico de Proteção de Dados para apresentação e aprovação da proposta de "Programa de Governança em Privacidade".	365	Ter 27/02/24	Qui 27/2/25
1.2.2	"Política de Proteção de Dados Pessoais"	–	Ter 27/02/24	Ter 27/02/24
1.3	**Tutela Coletiva de Proteção de Dados Pessoais**			
1.3.1	Indicação dos órgãos de execução com atribuição para a tutela coletiva de proteção de dados pessoais (Art. 159)	90	Ter 27/02/24	Qui 09/05/24

DESCRIÇÃO		DIAS	INÍCIO	TÉRMINO
1.4	**Maturidade da Instituição**			
1.4.1	Preencher o Relatório de Conformidade e encaminhar à UEPDAP (art. 161)	120	Ter 27/02/24	Ter 18/06/24
1.5	**Medidas de Segurança**			
1.5.1	Adotar medidas para a continuidade do resguardo do sigilo dos dados pessoais antes do desligamento dos integrantes (art. 125)	730	Ter 27/02/24	Qua 25/02/26
1.5.2	Definir e implantar o Termo de Compromisso de Manutenção de Sigilo (art. 124)	730	Ter 27/02/24	Qua 25/02/26
1.6	**Estrutura Organizacional para a Governança e Gestão da Proteção de Dados Pessoais**			
1.6.1	Constituir Estrutura Administrativa (Apoio técnico, jurídico e administrativo) (art. 155, parágrafo único c/c art. 45, § 3°)	365	Ter 27/02/24	Ter 27/02/24
1.6.2	Definir e implementar canal eletrônico de recebimento e para resposta com esclarecimentos de reclamações e comunicações dos titulares dos dados pessoais, e das comunicações da UEPDAP (art. 76, I)	730	Ter 27/02/24	Ter 27/02/24
1.6.3	Definir e implementar sistema eletrônico de organização, armazenamento e encaminhamento das reclamações e comunicações dos titulares dos dados pessoais e das comunicações da UEPDAP (art. 76, II)	730	Ter 27/02/24	Qui 27/02/25
1.7	**Inventário de Dados Pessoais**			
1.7.1	Realizar o mapeamento/inventário das bases de dados, abrangendo todos os dados pessoais da Unidade (art. 80 e seguintes)	730	Ter 27/02/24	Qua 25/02/26
1.7.2	Definir critérios de gestão de riscos (art. 136)	730	Ter 27/02/24	Qua 25/02/26
1.8	**Levantamento dos contratos relacionados a Dados Pessoais**			
1.8.1	Com base no mapeamento, identificar os contratos que tem por objeto serviços que tratam de dados pessoais, para que posteriormente tenham suas cláusulas adequadas conforme a Lei Geral de Proteção de Dados (Item 2.5.1 deste cronograma).	365	Ter 27/02/24	Ter 25/02/25
2	**Construção e Execução**			
2.1	**Políticas e práticas para proteção da privacidade do cidadão**			
2.1.1	Desenvolver plano de comunicação, para atendimento do público interno e externo, por meio dos órgãos de comunicação social, da Política de Proteção de Dados Pessoais e da Política Nacional de Proteção de Dados Pessoais (art. 166)	365	Ter 27/02/24	Ter, 25/02/25

DESCRIÇÃO		DIAS	INÍCIO	TÉRMINO
2.1.2	Desenvolver plano de comunicação, para atendimento do público interno e externo, por meio dos órgãos de comunicação social, da Política de Proteção de Dados Pessoais e da Política Nacional de Proteção de Dados Pessoais (art. 166)	365	Ter 27/02/24	Ter 25/02/25
2.2	**Cultura de segurança e proteção de dados e Privacidade desde a Concepção (privacy by design)**			
2.2.1	Assegurar, quando da implantação e adequação dos projetos, processos, sistemas, banco de dados, serviços e produtos, atuais e futuros, desde a concepção e durante todo o ciclo de vida, que eles contenham mecanismos de segurança e proteção de dados, inclusive nos treinamentos de usuários, design, codificação, testes e manutenção (art.. 126 e seguintes)	730	Ter 27/02/24	Qua 25/02/26
2.3	**Relatório de Impacto à Proteção de Dados Pessoais (RIDP)**			
2.3.1	Elaborar o Relatório de Impacto à Proteção de Dados Pessoais (art. 137)	730	Ter 27/02/24	Qua 25/02/26
2.4	**2.4 Medidas e Política de Segurança da Informação e Política de Proteção de Dados Pessoais**			
2.4.1	Definir a "Política de Segurança da Informação"	730	Ter 27/02/24	Qua 25/02/26
2.4.2	Definir o "Programa em Privacidade de Dados" (mencionado no art. 132, IV)	365	Ter 27/02/24	Qui 27/2/25
2.4.3	Definir a "Política de Proteção de Dados Pessoais" (mencionado no art. 132, IV)	-	Ter 27/02/24	Ter 27/02/24
2.4.4	2.4.4 Garantir o armazenamento de dados internos em bases específicas, com reforço de proteção, pseudonimização e criptografia (art. 107)	730	Ter 27/02/24	Qua 25/02/26
2.4.5	Adotar medidas técnicas e administrativa de proteção de dados, como a minimização, pseudonimização, etc. (art. 127)	730	Ter 27/02/24	Qua 25/02/26
2.4.6	Decidir sobre o uso compartilhado de dados pessoais (art. 38, IV)	730	Ter 27/02/24	Qua,25/02/26
2.4.7	Definir modelo para reclamações ou pedido de informações relativas às ofensas à proteção dos dados pessoais dos membros, servidores, estagiários e prestadores de serviços da Unidade do Ministério Público (art. 109)	730	Ter 27/02/24	Qua 25/02/26
2.5	**Adequação de Cláusulas Contratuais**			
2.5.1	Adequar os contratos e convênios para definir responsabilidades de controladores, operadores e eventuais terceiros (art. 68 c.c. art. 171 e art. 146, parágrafo único)	365	Ter 27/02/24	Ter 25/02/25

DESCRIÇÃO		DIAS	INÍCIO	TÉRMINO
2.6	**Termos de Uso e Política de Privacidade**			
2.6.1	Definir "Política de Privacidade"	-	Ter 27/02/24	Ter 27/02/24
2.6.2	Publicar no sítio a "Política de Privacidade", com a descrição de hipóteses em que se realiza o tratamento de dados pessoais (art. 65, parágrafo único e 132, III)	-	Ter 27/02/24	Ter 27/02/24
2.6.3	Descrever no site as informações a respeito da política de coleta e gestão do consentimento dos usuários, quanto ao uso de cookies ou tecnologias similares "Política de Cookies" (art. 133, parágrafo único)	-	Ter 27/02/24	Ter 27/02/24
2.7	**Instruções de Serviço**			
2.7.1	Expedir "instruções de serviços", em especial quanto às normas de segurança, os padrões técnicos e obrigações específicas (art. 38, I)	730	Ter 27/02/24	Qua 25/02/26
2.7.2	Adequar todos os atos internos (Art. 156)	365	Ter 27/02/24	Qui 27/2/25
2.8	**Sistemas Informatizados**			
2.8.1	Descrever nos sistemas a previsão legal, a finalidade, os procedimentos e práticas utilizadas no tratamento de dados pessoas nos sistemas informatizados (art. 132)	730	Ter 27/02/24	Qua 25/02/26
2.8.2	Descrever nos sistemas as informações a respeito da política de coleta e gestão do consentimento dos usuários, quanto ao uso de cookies ou tecnologias similares (art. 133, parágrafo único)	730	Ter 27/02/24	Qua 25/02/26
2.8.3	Implementar mecanismos de controle, identificação e registro de acesso do usuário a dados pessoais que sejam disponibilizados por sistemas informatizados (art. 134)	730	Ter 27/02/24	Qua 25/02/26
2.8.4	mplementar mecanismos de controle, identificação e registro de acesso do usuário a dados pessoais que sejam disponibilizados por sítio eletrônico (art. 134)	730	Ter 27/02/24	Qua 25/02/26
2.9	**Capacitação**			
2.9.1	Implementar e adequar programas de treinamento de usuários (art. 126, §2°)	-	Ter 27/02/24	Ter 27/02/24
2.9.2	Orientar as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos (art. 38, II)	-	Ter 27/02/24	Ter 27/02/24
3	**Monitoramento**			
3.1	**Indicadores de Performance**			
3.1.1	Definir os indicadores de desempenho, para identificar as lacunas do Programa de Governança em Privacidade assim como o status de outras iniciativas de privacidade.	365	Ter 27/02/24	Qui 27/2/25

DESCRIÇÃO		DIAS	INÍCIO	TÉRMINO
3.2	**Gestão de Incidentes**			
3.2.1	Definir o modelo de Gestão de Incidentes, que conte com um planejamento de resposta a incidentes e que registre o incidentes de segurança da informação e de privacidade.	-	Ter 27/02/24	Ter 27/02/24
3.3	**Análise de resultados**			
3.3.1	Analisar os resultados obtidos do monitoramento dos indicadores de performance, verificando o atingimento de metas e sugerindo medidas para o aperfeiçoamento do modelo de proteção de dados	730	Ter 27/02/24	Qua 25/02/26
3.4	**Reporte de Resultados**			
3.4.1	Reportar à Alta Administração os resultados obtidos, por meio do CEPDAP, viabilizando a manutenção do patrocínio para a manutenção do Programa	365	Ter 27/02/24	Qui 27/2/25

MPF
Ministério Público Federal