



Sumário

Ministério da Fazenda.....1

Ministério da Justiça e Segurança Pública1

Ministério do Meio Ambiente e Mudança do Clima.....4

Ministério da Previdência Social4

Ministério da Saúde.....4

.....Esta edição é composta de 6 páginas

Ministério da Fazenda

GABINETE DO MINISTRO

PORTARIA MF Nº 2.198, DE 23 DE JULHO DE 2026

Estabelece o valor da subvenção econômica da Gasolina "A", para fins do disposto no art. 1º da Medida Provisória nº 1.358, de 13 de maio de 2026.

O MINISTRO DE ESTADO DA FAZENDA, no uso das atribuições que lhe confere o art. 87, parágrafo único, inciso II, da Constituição, e tendo em vista o disposto no art. 1º, § 2º, da Medida Provisória nº 1.358, de 13 de maio de 2026, resolve:

Art. 1º O valor unitário da subvenção econômica a ser paga aos beneficiários de que trata o art. 1º da Medida Provisória nº 1.358, de 13 de maio de 2026, referente à comercialização de Gasolina "A", fica estabelecido em R\$ 0,44 (quarenta e quatro centavos de real) por litro de Gasolina "A".

§ 1º O pagamento da subvenção econômica ao beneficiário não poderá superar o ônus relativo à incidência das alíquotas de tributos federais aplicáveis à produção e à importação dos combustíveis subvencionados.

§ 2º A subvenção econômica de que trata o caput terá vigência por trinta dias, a contar de 26 de julho de 2026.

Art. 2º Esta Portaria entra em vigor em 26 de julho de 2026.

DARIO CARNEVALLI DURIGAN

Ministério da Justiça e Segurança Pública

GABINETE DO MINISTRO

PORTARIA MJSP Nº 1.248, DE 23 DE JULHO DE 2026

Institui o Programa Nacional de Integração e Compartilhamento de Dados e Informações para a Segurança Pública e Defesa Social - Infoseg, estabelece diretrizes para a consolidação da Base Nacional de Segurança Pública como componente estratégico da arquitetura do Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas - Sinesp e dispõe sobre a governança dos eixos estratégicos de gestão e constituição de dados e de uso, consulta e disponibilização controlada de informações no âmbito do Ministério da Justiça e Segurança Pública.

O MINISTRO DE ESTADO DA JUSTIÇA E SEGURANÇA PÚBLICA, no uso das atribuições que lhe confere o art. 87, parágrafo único, incisos I e II, da Constituição, tendo em vista o disposto na Lei Complementar nº 101, de 4 de maio de 2000, na Lei nº 12.527, de 18 de novembro de 2011, na Lei nº 13.675, de 11 de junho de 2018, na Lei nº 13.709, de 14 de agosto de 2018, na Lei nº 14.129, de 29 de março de 2021, na Lei nº 14.600, de 19 de junho de 2023, no Decreto nº 9.489, de 30 de agosto de 2018, no Decreto nº 10.046, de 9 de outubro de 2019, no Decreto nº 12.572, de 4 de agosto de 2025, na Portaria MJSP nº 2, de 28 de janeiro de 2022, na Resolução ConSinesp/MJSP nº 1, de 17 de junho de 2021, e o que consta do Processo Administrativo nº 08020.006787/2026-34, resolve:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º Instituir, no âmbito do Ministério da Justiça e Segurança Pública, o Programa Nacional de Integração e Compartilhamento de Dados e Informações para a Segurança Pública e Defesa Social - Infoseg com a finalidade de promover a integração de dados e informações de interesse da segurança pública e defesa social.

§ 1º O Programa tem por objetivo apoiar a formulação, a implementação, a execução, o monitoramento e a avaliação da Política Nacional de Segurança Pública e Defesa Social e está inserido na Política de Integração de Dados e Informações de Interesse da Segurança Pública constante da Carteira de Políticas Públicas do Ministério da Justiça e Segurança Pública.

§ 2º O Programa será executado sem prejuízo das competências constitucionais, legais e regulamentares dos órgãos e das entidades controladores, gestores, custodiantes ou responsáveis pelas bases de dados ou informações eventualmente integradas, consultadas ou compartilhadas.

§ 3º O Programa será estruturado em eixos de Ingestão e Constituição de Dados e de Uso, Consulta e Disponibilização Controlada de Informações, operacionalizados por projetos e iniciativas regidos por instrumentos próprios, de acordo com seu escopo, duração e finalidade.

§ 4º Os projetos, as iniciativas e os instrumentos vinculados ao Programa dependerão de análise técnica e, quando cabível, de análise jurídica específica, observado o regime próprio da base, do sistema, do serviço ou da informação envolvida.

Art. 2º Para os fins desta Portaria, considera-se:

I - dado: unidade mínima de informação, estruturada ou não estruturada, relacionada a evento, registro, pessoa, objeto, unidade, procedimento, atendimento, despacho, recurso, ocorrência, investigação, atividade administrativa ou outro elemento de interesse da segurança pública;

II - informação: conjunto de dados ordenados, contextualizados e interpretáveis, aptos a produzir significado para fins de gestão, planejamento, estatística, inteligência, investigação, controle, transparência ou avaliação de políticas públicas;

III - Base Nacional de Segurança Pública: componente estratégico da arquitetura do Sinesp, constituído como ambiente nacional integrado de recepção, integração, validação, auditoria, monitoramento, consolidação, disponibilização controlada e governança de dados e informações de interesse da segurança pública e defesa social, mantido pelo Ministério da Justiça e Segurança Pública, por intermédio da Diretoria de Gestão e Integração de Informações da Secretaria Nacional de Segurança Pública, observados o regime jurídico aplicável e as competências do Conselho Gestor do Sinesp;

IV - Sinesp: Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas, instituído pela Lei nº 13.675, de 11 de junho de 2018, como meio e instrumento para implementação da Política Nacional de Segurança Pública e Defesa Social;

V - integração de dados: conjunto de processos técnicos, jurídicos e administrativos destinados a viabilizar interoperabilidade, consulta, transmissão, recepção, atualização, correlação ou uso qualificado de dados entre sistemas, bases ou plataformas;

VI - compartilhamento qualificado de dados: disponibilização, comunicação, interconexão, consulta ou transferência de dados entre órgãos, entidades públicas, entes federados ou, quando admitido pela legislação aplicável e por instrumento específico, pessoas jurídicas de direito privado, sempre para finalidade determinada, mediante controles de acesso, segurança, rastreabilidade, auditoria e responsabilização;

VII - órgão gestor, controlador ou custodiante: órgão, entidade ou pessoa jurídica responsável, conforme a legislação aplicável, pela governança, custódia, administração, segurança, autorização de acesso ou definição das condições de uso de determinada base de dados ou informações;

VIII - ente federado aderente: Estado, Distrito Federal ou Município que formalize adesão ao Programa, observadas as condições desta Portaria e dos instrumentos jurídicos ou técnicos aplicáveis;

IX - matriz de dados: documento técnico que identifica bases, categorias de dados, atributos, metadados, finalidades, fontes, periodicidade, qualidade, formato, sensibilidade, restrições de uso e demais condições aplicáveis a determinada integração, consulta, disponibilização ou compartilhamento;

X - matriz de acesso: documento técnico que define perfis, níveis, escopos, finalidades, credenciais, requisitos de autenticação, autorização, auditoria, restrições de uso e condições de revisão dos acessos concedidos;

XI - redisseminação: transferência, comunicação, disponibilização, replicação ou concessão de acesso a dados ou informações a terceiro não originalmente autorizado no instrumento jurídico ou técnico aplicável;

XII - serviço de dados de alto impacto: serviço, integração, consulta, cruzamento ou disponibilização que, em razão do volume, da sensibilidade, da criticidade operacional, da natureza biométrica, genética, georreferenciada ou identificável dos dados, do uso de automação decisória, perfilamento, tecnologias de identificação ou cruzamento massivo de bases possa gerar risco relevante à segurança pública, à segurança da sociedade ou do Estado, à privacidade, às liberdades civis ou a outros direitos fundamentais; e

XIII - usuário autorizado: agente público, profissional credenciado, unidade institucional, sistema, aplicação ou serviço que possua permissão formal para acessar, consultar, integrar, transmitir, receber ou tratar dados ou informações no âmbito do Programa, nos limites da finalidade, do perfil de acesso e do instrumento aplicável.

Parágrafo único. As referências a controlador, operador, gestor, custodiante, recebedor, solicitante ou usuário de dados serão interpretadas conforme a legislação aplicável ao caso concreto, especialmente a legislação de proteção de dados pessoais, de acesso à informação, de segurança pública, de segurança da informação, de inteligência, de investigação e de compartilhamento de dados no âmbito da administração pública.

CAPÍTULO II

DOS OBJETIVOS E DAS DIRETRIZES

Art. 3º São objetivos do Programa:

I - consolidar a Base Nacional de Segurança Pública como componente estratégico da arquitetura do Sinesp e estruturar a infraestrutura técnica, institucional, jurídica e de governança necessária ao seu funcionamento;

II - fortalecer a integração nacional de dados e informações de interesse da segurança pública e defesa social;

III - ampliar, de forma segura, proporcional e juridicamente adequada, a interoperabilidade entre sistemas, bases de dados, serviços, imagens, sinais, alertas e indicadores de interesse da segurança pública;

IV - estruturar ambiente nacional de articulação técnica e institucional para disponibilização de serviços de dados aos órgãos integrantes do Sistema Único de Segurança Pública;

V - apoiar a formulação, a implementação, a execução, o monitoramento e a avaliação de políticas públicas de segurança pública e defesa social baseadas em evidências, diagnósticos e estatísticas validadas;

VI - subsidiar ações de prevenção e repressão qualificada da criminalidade, respeitadas as atribuições legais dos órgãos competentes;

VII - aprimorar a qualidade, a completude, a tempestividade, a rastreabilidade, a comparabilidade e a consistência dos dados de segurança pública e defesa social;

VIII - fomentar a padronização, a interoperabilidade federada e a qualificação dos registros relacionados à atividade-fim e à gestão das instituições de segurança pública; e

IX - promover o uso responsável, seguro, auditável e proporcional de dados e informações, observadas as restrições legais, os regimes jurídicos especiais e os direitos e as garantias fundamentais.

Art. 4º O Programa observará, entre outras, as seguintes diretrizes:

I - legalidade, finalidade, adequação, necessidade, proporcionalidade, segurança, prevenção, responsabilização e prestação de contas;

II - respeito à proteção constitucional dos dados pessoais, à intimidade, à vida privada, à honra, à imagem, ao sigilo legal e às restrições de acesso previstas em lei;

III - interoperabilidade de sistemas, preferencialmente por meio de consulta qualificada, serviços controlados de dados, interfaces de programação de aplicações, documentos de interoperabilidade ou outros mecanismos técnicos seguros;

IV - controle de acesso baseado em perfil funcional, atributos institucionais, finalidade, nível de sensibilidade da informação, necessidade de conhecer e atribuição legal do usuário;

V - registro, rastreabilidade, auditabilidade e monitoramento dos acessos, consultas, integrações, transmissões, recepções e demais operações de tratamento;

VI - responsabilização administrativa, civil e penal pelo acesso, uso, compartilhamento, armazenamento, divulgação, redisseminação ou tratamento indevido de dados e informações;

VII - condicionamento do acesso aos dados à observância da reciprocidade no processo de alimentação da Base Nacional de Segurança Pública, a ser realizada de forma regular e tempestiva, em conformidade com os critérios de qualidade, completude e integralidade estabelecidos pela Diretoria de Gestão e Integração de Informações;

VIII - preservação da autonomia e das competências dos órgãos e das entidades gestores, controladores ou custodiantes das bases de dados;

IX - segregação de funções, revisão periódica de acessos, autenticação compatível com o risco e adoção de mecanismos de prevenção, detecção e resposta a incidentes;

X - transparência institucional em camadas, observadas as restrições legais, a segurança da informação, a proteção de dados pessoais e a preservação de atividades de inteligência, investigação, fiscalização e segurança pública; e

XI - observância das competências do Conselho Gestor do Sinesp quanto a diretrizes, metodologia, padronização, categorias, regras de tratamento, padrões de interoperabilidade, critérios de integração e níveis de acesso relativos ao Sinesp.

CAPÍTULO III

DA COORDENAÇÃO E DA GOVERNANÇA

Art. 5º O Programa será coordenado pela Secretaria Nacional de Segurança Pública do Ministério da Justiça e Segurança Pública.

§ 1º A coordenação técnica do Programa caberá à Diretoria de Gestão e Integração de Informações da Secretaria Nacional de Segurança Pública, sem prejuízo das competências das demais unidades do Ministério da Justiça e Segurança Pública.

§ 2º A execução do Programa não afastará a observância das normas específicas incidentes sobre cada base, sistema, serviço ou informação, inclusive quanto a sigilo, segredo de justiça, proteção de dados pessoais, informações pessoais, informações classificadas, inteligência financeira, inteligência de segurança pública, dados fiscais, dados



§ 3º A Diretoria de Gestão e Integração de Informações da Secretaria Nacional de Segurança Pública poderá realizar inventário dos instrumentos vigentes de que trata o caput, com a finalidade de identificar bases integradas, órgãos partícipes, finalidades autorizadas, perfis de acesso, requisitos de segurança, prazos de vigência, limitações de uso e eventuais necessidades de adequação às diretrizes desta Portaria.

§ 4º Os instrumentos vigentes poderão ser progressivamente adequados às diretrizes do Programa, especialmente quanto à matriz de dados, matriz de acesso, controle de usuários, rastreabilidade, auditoria, proteção de dados pessoais, segurança da informação, resposta a incidentes, redisseminação e responsabilização pelo uso indevido.

Art. 18. As novas integrações, consultas, disponibilizações e os novos compartilhamentos no âmbito do Programa poderão ser formalizados por meio de:

I - acordo de cooperação técnica;

II - convênio;

III - termo de execução descentralizada, quando cabível;

IV - protocolo de intenções;

V - termo de compartilhamento de dados;

VI - documento de interoperabilidade;

VII - plano de trabalho;

VIII - termo de adesão;

IX - termo de responsabilidade e confidencialidade;

X - contrato, quando cabível; ou

XI - outro instrumento jurídico ou técnico admitido pela legislação aplicável.

Art. 19. O instrumento a que se refere o art. 18 conterá, no mínimo, quando aplicável:

I - identificação das partes;

II - objeto;

III - finalidade;

IV - fundamento jurídico;

V - bases, sistemas, serviços, dados, imagens, sinais, alertas, indicadores ou informações abrangidos;

VI - categorias de dados;

VII - forma de acesso, consulta, integração ou disponibilização;

VIII - público autorizado;

IX - perfis de acesso;

X - possibilidade ou vedação de acesso por entes federados aderentes;

XI - possibilidade ou vedação de redisseminação;

XII - responsabilidades das partes;

XIII - medidas de segurança da informação;

XIV - regras de sigilo e confidencialidade;

XV - regras de auditoria e fiscalização;

XVI - prazo de vigência;

XVII - prazo de retenção, descarte ou eliminação dos dados;

XVIII - hipóteses de suspensão, bloqueio, revogação ou encerramento;

XIX - regras de comunicação de incidentes;

XX - regras de responsabilização por uso indevido;

XXI - papéis e responsabilidades dos agentes envolvidos, inclusive quanto à governança, custódia, operação, segurança e autorização de uso dos dados;

XXII - matriz de dados e matriz de acesso;

XXIII - critérios de revisão periódica, recertificação de usuários, revogação de credenciais e cancelamento de acessos;

XXIV - restrições ao enriquecimento, à cópia local, à extração massiva, à redisseminação ou ao uso para finalidade diversa; e

XXV - plano de resposta a incidentes, quando cabível.

Art. 20. A formalização de instrumentos que envolvam dados pessoais, dados pessoais sensíveis, dados sigilosos, informações classificadas, imagens, dados biométricos, dados genéticos, bases estratégicas, bases privadas, cruzamento massivo de bases, tecnologias de identificação, perfilamento, decisão automatizada ou serviços de dados de alto impacto deverá ser precedida de análise técnica, avaliação de risco e, quando cabível, de relatório de impacto à proteção de dados pessoais ou documento equivalente, bem como de análise de conformidade normativa pelas unidades competentes, sem prejuízo de manifestação da Consultoria Jurídica junto ao Ministério da Justiça e Segurança Pública nos processos submetidos à sua apreciação.

§ 1º A avaliação de risco de que trata o caput deverá considerar, no mínimo, a finalidade, a necessidade, a proporcionalidade, a sensibilidade dos dados, o volume de informações, os perfis de acesso, as hipóteses de redisseminação, as medidas de segurança, os riscos aos direitos fundamentais, os impactos à segurança pública e as medidas de mitigação aplicáveis.

§ 2º A formalização de instrumentos que envolvam serviços de dados de alto impacto, na forma do art. 2º, inciso XII, será precedida, obrigatoriamente, de relatório de impacto à proteção de dados pessoais ou documento equivalente, sendo, nas demais hipóteses de que trata o caput, elaborado relatório quando a avaliação de risco assim o indicar.

§ 3º A participação de pessoa jurídica de direito privado em instrumento vinculado ao Programa terá caráter instrumental, na condição de fornecedora, cooperadora, prestadora de serviço ou disponibilizadora de dados, imagens, sinais, alertas, indicadores ou soluções tecnológicas de interesse da segurança pública, não lhe conferindo direito de acesso aos dados, bases, sistemas, serviços ou informações constantes do Programa, nem autorização para utilização de dados públicos ou compartilhados para finalidade privada, comercial, mercadológica ou incompatível com o interesse público autorizado.

§ 4º É vedado conferir a pessoa jurídica de direito privado tratamento, gestão, custódia ou acesso irrestrito à totalidade de banco de dados de segurança pública, sem prejuízo de serviços técnicos específicos, proporcionais, segmentados e supervisionados por órgão ou entidade pública, quando admitidos pela legislação aplicável e pelo instrumento próprio.

§ 5º Na hipótese de contratação de pessoa jurídica de direito privado para prestação de serviço técnico, tecnológico ou operacional relacionado ao Programa, eventual tratamento de dados necessário à execução contratual ficará restrito aos limites do contrato, do instrumento aplicável e das instruções do órgão público responsável, vedado o uso próprio, autônomo, irrestrito ou para finalidade diversa da autorizada.

§ 6º O relatório de impacto à proteção de dados pessoais ou documento equivalente será elaborado com a participação do encarregado pelo tratamento de dados pessoais do Ministério da Justiça e Segurança Pública, sem prejuízo da atuação das unidades técnicas competentes.

Art. 21. A participação dos Estados, do Distrito Federal e dos Municípios, bem como de seus órgãos, suas entidades, suas instituições e seus usuários autorizados, nas iniciativas, nas soluções e nos serviços controlados de dados vinculados ao Programa observará os instrumentos vigentes ou futuros, os termos de adesão, os documentos de interoperabilidade, os credenciamentos, as normas das soluções do Sinesp e as demais condições técnicas e jurídicas aplicáveis.

§ 1º A participação de que trata o caput não autoriza, por si só, acesso automático, irrestrito, massivo, permanente ou genérico a todas as bases, sistemas, serviços ou informações vinculados ao Programa.

§ 2º O acesso aos serviços controlados de dados dependerá de finalidade autorizada, perfil de acesso, matriz de acesso, necessidade de conhecer, requisitos de segurança, rastreabilidade, auditoria e condições estabelecidas no instrumento jurídico ou técnico aplicável.

§ 3º Quando o instrumento firmado pelo Ministério da Justiça e Segurança Pública ou pela Secretaria Nacional de Segurança Pública com o órgão, a entidade ou pessoa jurídica gestora, controladora ou custodiante autorizar o acesso pelos entes federados ou por seus órgãos, suas entidades, suas instituições ou seus usuários autorizados, a habilitação poderá ocorrer pelos fluxos de credenciamento, termos de adesão, regras da solução, matriz de acesso e auditoria definidos no âmbito do Programa, dispensada a celebração de novo instrumento individual com cada ente federado, salvo exigência legal, regulamentar ou do próprio órgão, entidade ou pessoa jurídica gestora, controladora ou custodiante.

Art. 22. O termo de adesão de ente federado ao Programa deverá prever, no mínimo, quando aplicável:

I - identificação da autoridade competente e das unidades responsáveis;

II - bases, sistemas, serviços ou informações abrangidos;

III - finalidades autorizadas;

IV - responsabilidades do ente aderente quanto à qualidade, atualização, integridade e segurança dos dados;

V - regras de gestão de usuários, perfis de acesso, credenciais, revisão periódica e desligamento;

VI - requisitos de auditoria, rastreabilidade, sigilo, confidencialidade e resposta a incidentes;

VII - condições de suporte, interoperabilidade, continuidade, reversibilidade e encerramento; e

VIII - hipóteses de suspensão, bloqueio, revogação ou restrição de acesso em caso de irregularidade, incidente, desvio de finalidade ou descumprimento do instrumento.

CAPÍTULO VI

DA TRANSPARÊNCIA, DO CONTROLE E DA AUDITORIA

Art. 23. A Secretaria Nacional de Segurança Pública manterá registro atualizado das iniciativas de integração, consulta, disponibilização e compartilhamento de dados no âmbito do Programa, observadas as restrições legais de sigilo, proteção de dados pessoais, segurança da informação e preservação de atividades de inteligência, investigação ou fiscalização.

§ 1º O registro de que trata o caput poderá ser organizado em versão administrativa, de acesso restrito, e versão pública, com informações institucionais, agregadas ou suprimidas na medida necessária à proteção de dados pessoais, informações sigilosas, informações classificadas, segurança de sistemas, atividades de inteligência, investigação, fiscalização e segurança pública.

§ 2º O registro administrativo deverá subsidiar a gestão, a auditoria, o monitoramento, a avaliação de riscos e a prestação de contas do Programa.

Art. 24. Sempre que juridicamente possível, deverão ser disponibilizadas informações institucionais sobre o Programa, inclusive quanto a finalidades, governança, bases normativas, órgãos participantes, instrumentos celebrados e mecanismos de controle.

Parágrafo único. A transparência de que trata o caput não abrangerá informações cuja divulgação possa comprometer a segurança da sociedade ou do Estado, atividades de inteligência, investigação ou fiscalização em andamento, sigilo legal, segurança de sistemas, dados pessoais, dados sigilosos, informações classificadas ou restrições justificadas por órgão, entidade ou pessoa jurídica gestora, controladora ou custodiante, desde que compatíveis com a legislação aplicável, com o instrumento firmado e com o interesse público.

Art. 25. A Secretaria Nacional de Segurança Pública, por intermédio da Diretoria de Gestão e Integração de Informações, poderá realizar auditorias ordinárias ou extraordinárias nas integrações, nos acessos, nas consultas, nas disponibilizações e nos compartilhamentos realizados no âmbito do Programa.

§ 1º As soluções, as iniciativas e os serviços controlados de dados vinculados ao Programa deverão manter trilhas de auditoria compatíveis com o risco da operação, aptas a identificar, quando aplicável, o usuário, o órgão de origem, a data, o horário e o fuso horário, o serviço acessado, a operação realizada, a finalidade declarada e os demais elementos necessários à verificação de conformidade, nos termos do instrumento jurídico ou técnico aplicável e da regulamentação específica da solução.

§ 2º As auditorias poderão ter por objeto, entre outros aspectos, a regularidade dos acessos, a compatibilidade entre consulta e finalidade, a observância dos perfis de acesso, a segurança da informação, a aderência aos instrumentos firmados, a ocorrência de eventual desvio de finalidade, a existência de redisseminação não autorizada e o cumprimento das medidas de mitigação de risco.

§ 3º Constatados indícios de irregularidade, desvio de finalidade, acesso indevido, redisseminação não autorizada, incidente de segurança ou descumprimento das normas aplicáveis, a Secretaria Nacional de Segurança Pública adotará as providências necessárias à suspensão, ao bloqueio ou à restrição preventiva do acesso, à comunicação ao órgão ou à entidade de origem do usuário, à instauração de apuração administrativa e à comunicação aos órgãos competentes, quando cabível, observados, nas hipóteses de incidente cibernético ou de segurança da informação, os fluxos institucionais de prevenção, tratamento e resposta a incidentes cibernéticos do Ministério da Justiça e Segurança Pública.

§ 4º As medidas preventivas de que trata o § 3º poderão ser adotadas imediatamente quando houver risco à segurança da sociedade ou do Estado, à segurança pública, ao sigilo legal, à segurança de sistemas, à integridade das bases ou aos direitos fundamentais, sem prejuízo de posterior regularização procedimental.

§ 5º A interrupção injustificada no envio de dados ou a desconformidade com os critérios de totalidade e qualidade estabelecidos ensejará restrições de acesso ou medidas administrativas cabíveis, até que a regularidade seja homologada tecnicamente pela Diretoria de Gestão e Integração de Informações.

§ 6º As medidas previstas neste artigo não prejudicam a aplicação das consequências previstas no art. 37, §§ 2º e 4º, da Lei nº 13.675, de 11 de junho de 2018, observado o disposto no art. 19, inciso VIII, do Decreto nº 9.489, de 30 de agosto de 2018.

§ 7º O disposto neste artigo não afasta a competência privativa da Diretoria de Gestão e Integração de Informações para manter os registros de acessos e de atividades dos usuários e promover as auditorias necessárias relativas à solução Sinesp Infoseg, nos termos da Resolução ConSinesp/MJSP nº 1, de 17 de junho de 2021, sem prejuízo das competências dos órgãos de controle e demais instâncias competentes.

§ 8º As credenciais e os perfis de acesso concedidos no âmbito do Programa serão revistos em prazo não superior a doze meses, com revogação imediata das credenciais de usuários desligados, remanejados ou cuja necessidade de conhecer tenha cessado.

CAPÍTULO VII

DISPOSIÇÕES FINAIS

Art. 26. A execução do Programa observará a disponibilidade orçamentária e financeira do Ministério da Justiça e Segurança Pública e não implicará, por si só, criação de despesa obrigatória, criação de cargos, funções ou estruturas administrativas autônomas.

§ 1º As iniciativas, os projetos e os instrumentos vinculados ao Programa que demandem contratação, desenvolvimento tecnológico, integração sistêmica ou transferência ou descentralização de recursos serão precedidos de planejamento específico e da estimativa de impacto orçamentário-financeiro e da declaração de adequação orçamentária e financeira de que trata o art. 16 da Lei Complementar nº 101, de 4 de maio de 2000, observado o disposto no art. 8º.

§ 2º As iniciativas e os projetos vinculados ao Programa não criarão despesa obrigatória de caráter continuado sem a observância do art. 17 da Lei Complementar nº 101, de 4 de maio de 2000.

Art. 27. A Secretaria Nacional de Segurança Pública poderá expedir orientações técnicas complementares, manuais, protocolos, modelos de documentos, matrizes de dados, matrizes de acesso, termos de responsabilidade, termos de adesão e demais instrumentos necessários à execução desta Portaria, observadas as competências do Conselho Gestor do Sinesp e de demais órgãos e entidades competentes.

Art. 28. Os casos omissos serão dirimidos pela Secretaria Nacional de Segurança Pública, ouvido o Conselho Gestor do Sinesp quando a matéria se inserir em suas competências legais ou regulamentares e, quando cabível, a Consultoria Jurídica junto ao Ministério da Justiça e Segurança Pública ou outra instância competente.

Art. 29. Esta Portaria entra em vigor na data de sua publicação.

