RESOLUÇÃO GPGJ Nº 2.710, DE 29 DE MAIO DE 2025.

Revoga a Resolução GPGJ nº 2.548, de 29 de agosto de 2023, e estabelece novo Plano de Resposta e Remediação de Incidentes de Segurança de Dados do Ministério Público do Estado do Rio de Janeiro.

O **PROCURADOR-GERAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO**, no uso de suas atribuições legais,

CONSIDERANDO a previsão constitucional (art. 5º, LXXIX - incluído pela Emenda Constitucional nº 115, de 10 de fevereiro de 2022), as disposições da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), da Lei nº 12.965, de 23 de abril de 2014 (Lei do Marco Civil da *Internet*), da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), da Lei nº 8.625, de 12 de fevereiro de 1993 (Lei Orgânica Nacional do Ministério Público), da Lei Complementar Estadual nº 106, de 03 de janeiro de 2003 e da Resolução GPGJ nº 2.699, de 20 de maio de 2025, bem como as boas práticas de governança de dados e segurança da informação;

CONSIDERANDO que os responsáveis pelo tratamento de dados em desconformidade com a lei poderão incidir nas sanções do regime jurídico próprio, da Lei de Improbidade Administrativa, da Lei de Acesso à Informação e da Lei nº 13.709/2018;

CONSIDERANDO que o art. 46 da Lei Geral de Proteção de Dados Pessoais estabelece que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, e que tais medidas de segurança deverão ser observadas desde a concepção do produto ou serviço até a sua execução;

CONSIDERANDO que o art. 48 da Lei Geral de Proteção de Dados Pessoais e a Resolução do Conselho Diretor da Autoridade Nacional de Proteção de Dados (CD/ANPD) nº 15, de 24 de abril de 2024, preveem que o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares;

CONSIDERANDO que o art. 50 da mesma lei estabelece que controladores e operadores, no âmbito de suas competências, poderão formular regras de boas práticas de governança para o tratamento de dados pessoais; e o inciso I do § 2º do referido artigo dispõe que deve ser implementado um Programa de Governança em Privacidade que conte com planos de resposta a incidentes e remediação;

CONSIDERANDO que o art. 148 da Resolução nº 281, de 12 de dezembro de 2023, do Conselho Nacional do Ministério Público (CNMP), prevê que o controlador deverá comunicar à Unidade Especial de Proteção de Dados Pessoais (UEPDAP/CNMP) a ocorrência de incidente de segurança com possibilidade de causar dano relevante aos titulares;

CONSIDERANDO que a Resolução GPGJ nº 2.699/2025 prevê, em seu art. 5º, inciso VII, a elaboração de planos de resposta e remediação de incidentes de segurança de dados; e

CONSIDERANDO o que consta do Procedimento SEI nº 20.22.0001.0014551.2025-80,

RESOLVE

Capítulo I

Disposições Iniciais

Art. 1º - Constitui incidente de segurança, de acordo com a Autoridade Nacional de Proteção de Dados (ANPD), qualquer evento adverso confirmado, relacionado à violação

das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais.

Parágrafo único - Pode configurar incidente de segurança qualquer evento adverso relacionado à segurança dos ativos ou sistemas de computação ou das redes de computadores, como ataques eletrônicos (*hacking*) e infecção de *malwares*, além de eventos provenientes de situações corriqueiras e acidentais, como envio de *e-mail* contendo dados pessoais (planilhas com listas e informações pessoais, por exemplo) a destinatário impróprio ou equivocado; *laptop* ou celular de membro ou servidor furtado ou roubado; descarte inadequado de dados pessoais (arquivos físicos); acesso não autorizado a informações, dentre outros.

Capítulo II

Gestão de Incidentes de Segurança

Art. 2º - Caso ocorra incidente que coloque em risco a segurança de dados pessoais, devem ser realizados os seguintes procedimentos:

I - avaliar internamente o incidente com o objetivo de obter informações iniciais sobre impacto do evento, natureza, categoria e quantidade de titulares de dados pessoais afetados; categoria e quantidade de dados afetados, consequências do incidente para os titulares e a entidade, criticidade e probabilidade; além disso, é necessário preservar todas as evidências do incidente;

II - comunicar ao Encarregado pelo Tratamento de Dados Pessoais do Ministério Público a existência do incidente, caso envolva dados pessoais;

III - comunicar ao controlador do Ministério Público do Estado do Rio de Janeiro, nos termos da LGPD, a existência do incidente, caso envolva dados pessoais;

IV - comunicar à Secretaria de Tecnologia da Informação e de Comunicação (STIC), em caso de incidentes na infraestrutura de tecnologia de informação;

V - emitir o relatório final com todas as informações coletadas, as ações realizadas para o tratamento efetivo do evento e as considerações necessárias para promover a melhoria contínua no atendimento de incidentes e para atualizar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

§ 1º - A ocorrência de incidente que possa acarretar risco ou dano relevante aos titulares deverá ser comunicada à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular de dados pessoais, conforme art. 48 da LGPD e a Resolução CD/ANPD nº 15/2024, bem como ao Conselho Nacional do Ministério Público, conforme art. 38, inciso V, da Resolução CNMP nº 281/2023.

§ 2º - O incidente de segurança pode acarretar risco ou dano relevante aos titulares quando puder afetar significativamente seus interesses e direitos fundamentais e, cumulativamente, envolver, pelo menos, um dos seguintes aspectos:

I - dados pessoais sensíveis;

II - dados de crianças, de adolescentes ou de idosos;

III - dados financeiros;

IV - dados de autenticação em sistemas;

V - dados protegidos por sigilo legal, judicial ou profissional; ou

VI - dados em larga escala.

§ 3º - O incidente de segurança que possa afetar significativamente interesses e direitos fundamentais estará caracterizado, dentre outras situações, quando a atividade

de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

§ 4º - Considera-se incidente com dados em larga escala aquele que abranger número significativo de titulares, considerando, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica de localização dos titulares.

Art. 3º - É dever do membro, servidor, aluno-residente, estagiário, terceirizado ou colaborador do Ministério Público, que tenha ciência de evento que possa configurar incidente de segurança, comunicá-lo imediatamente ao Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP), via procedimento administrativo no Sistema Eletrônico de Informações (SEI), preenchendo o formulário disponível.

Art. 4º - É facultado a qualquer interessado que tenha ciência de evento que possa configurar um incidente de segurança, a comunicação ao Comitê Estratégico de Proteção de Dados Pessoais, via procedimento administrativo no Sistema Eletrônico de Informações (SEI), preenchendo o formulário disponível.

Art. 5º - Nas hipóteses dos artigos 3º e 4º desta Resolução, recomenda-se que o comunicante forneça, se possível, as seguintes informações:

I - nome completo, identidade, nº de inscrição no CPF/CNPJ, conforme o caso, telefone e *e-mail*;

II - descrição resumida do suposto incidente;

III - motivos pelos quais entende que o suposto incidente tenha relação com a gestão de dados do Ministério Público do Estado do Rio de Janeiro;

IV - data do suposto incidente ou data provável, caso não tenha certeza da data;

V - caso o comunicado não tenha sido feito imediatamente após o suposto incidente ou sua ciência, a justificativa para a demora;

VI - apontamento de dados pessoais dos quais seja titular, que o comunicante suspeita tenham sido atingidos pelo incidente, se houver;

VII - se possível for a identificação, o apontamento de dados pessoais de terceiros que o comunicante suspeita tenham sido atingidos pelo incidente, se houver;

VIII - se possível for a identificação, quantidade de titulares de dados pessoais que o comunicante estima tenham sido atingidos pelo incidente; e

IX - se possível for, a identificação e a natureza da relação entre os titulares de dados supostamente atingidos e o controlador.

Parágrafo único - Caso não seja possível fornecer tais informações no momento da comunicação, o comunicante deverá descrever o incidente imediatamente com as informações disponíveis, podendo complementar o reporte posteriormente.

Art. 6º - É dever do operador, em relação ao incidente de segurança, comunicar imediatamente ao Ministério Público, enquanto órgão controlador, no prazo máximo de 24 (vinte e quatro) horas da ciência ou suspeita da ocorrência de qualquer incidente que implique violação ou risco de violação de dados pessoais, realizando-se a notificação via procedimento administrativo no Sistema Eletrônico de Informações (SEI), preenchendo o formulário disponível, adotando, no mínimo, as seguintes ações:

I - descrever o incidente e a natureza dos dados pessoais afetados, as categorias e o número de titulares dos dados pessoais em questão;

II - fornecer informações sobre os titulares de dados pessoais envolvidos;

III - informar as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais;

IV - comunicar o nome e os detalhes de contato do encarregado ou responsável por proteção de dados pessoais do operador;

V - descrever as prováveis consequências e riscos relacionados ao incidente de segurança;

VI - descrever as medidas adotadas ou propostas para solucionar o incidente de segurança; e

VII - descrever as medidas que foram ou serão tomadas para reverter ou mitigar os efeitos das perdas relacionadas ao incidente de segurança.

§ 1º - Qualquer não cumprimento, ainda que suspeito, das disposições legais relativas à proteção de dados pessoais pelo operador, seus funcionários, ou terceiros autorizados, acarretará a imposição de pena de multa de até 2% (dois por cento) do faturamento da empresa, a ser aplicada pela Autoridade Nacional de Proteção de Dados (ANPD), na forma do art. 52, inciso II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais).

§ 2º - A critério do Encarregado pelo Tratamento de Dados Pessoais do Ministério Público do Estado do Rio de Janeiro, o operador poderá ser provocado a colaborar na elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), conforme a sensibilidade e o risco inerente dos serviços objeto do eventual contrato firmado entre operador e controlador, no tocante a dados pessoais.

Art. 7º - Caso a comunicação não contenha todos os requisitos previstos nos artigos 5º ou 6º, conforme o caso, desta Resolução, o Comitê Estratégico de Proteção de Dados Pessoais poderá solicitar ao comunicante a complementação das informações no prazo de 24 (vinte e quatro) horas.

Art. 8º - Após verificar o preenchimento dos requisitos do art. 5º ou 6º, conforme o caso, desta Resolução, o Encarregado pelo Tratamento de Dados Pessoais deverá avaliar a veracidade e relevância do incidente, e, caso entenda que há elementos suficientes que possam comprovar a possibilidade de vazamento de dados, enviará o procedimento à Secretaria de Tecnologia da Informação e de Comunicação, para confirmação do possível vazamento e início da fase de triagem, análise e resposta.

Art. 9º - A Secretaria de Tecnologia da Informação e de Comunicação apresentará parecer sobre a possibilidade de comprovação do incidente reportado, e, em caso de confirmação, apresentará relatório do incidente ao Comitê Estratégico de Proteção de Dados Pessoais, do qual deverão constar:

I - a data e hora da detecção do incidente;

II - a data e hora do incidente e sua duração;

III - a vulnerabilidade explorada no evento, abrangendo situações como acesso indevido aos dados pessoais; roubo de dados; ataques cibernéticos; erros de programação de aplicativos e sistemas internos; engenharia social; descartes indevidos; repasse de dados pessoais; roubo, venda e utilização de dados tutelados pela entidade; comprometimento de senhas de acesso;

IV - a fonte dos dados pessoais, assim considerado o meio pelo qual foram obtidos os dados pessoais, tais como preenchimento de formulário eletrônico ou não eletrônico por parte do titular, API, uso compartilhado de dados, XML e *cookies*;

V - a extensão do vazamento, assim considerada a descrição dos dados pessoais e as informações afetadas, tais como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados;

VI - a indicação sobre a afetação de dados sensíveis, assim considerado o dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

VII - a indicação sobre a afetação de indivíduos vulneráveis, como crianças, adolescentes ou idosos;

VIII - o resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento;

IX - a avaliação do impacto, abrangendo possíveis consequências e efeitos negativos, incluindo a indicação ou estimativa de quão facilmente podem vir a ser identificados os titulares de dados atingidos pelo incidente;

X - a avaliação do impacto para a Instituição, como perda de confiabilidade do cidadão, ações judiciais, danos à imagem do Ministério Público em âmbito nacional e internacional, e impacto total ou parcial nas atividades desenvolvidas;

XI - o resumo das medidas técnicas implementadas até o momento para controlar os possíveis danos, bem como dos planos de ação para mitigação e correção;

XII - a indicação das lições aprendidas com a resolução do incidente;

XIII - possíveis problemas de natureza transfronteiriça; e

XIV - outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

Parágrafo único - A Secretaria de Tecnologia da Informação e de Comunicação deverá apresentar relatório com a maior brevidade possível e, de preferência, no prazo indicativo de 1 (um) dia útil, contado da data do conhecimento do incidente, sem prejuízo de posterior complementação.

Art. 10 - Recebido o relatório da Secretaria de Tecnologia da Informação e de Comunicação, e coletada as demais informações necessárias, o Encarregado pelo Tratamento de Dados Pessoais do Ministério Público do Estado do Rio de Janeiro comunicará à Autoridade Nacional de Proteção de Dados (ANPD) a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante.

§ 1º - A avaliação acerca da relevância do risco ou dano será feita com cautela e em atenção aos princípios da prevenção, responsabilização e prestação de contas, de modo que, em caso de dúvida, a comunicação à ANPD deverá ser realizada.

§ 2º - A ANPD, o CNMP e os titulares de dados pessoais deverão ser notificados nas hipóteses em que for confirmado que o incidente de segurança tenha afetado dados pessoais e que pode acarretar risco ou dano relevante ao titular destes dados, respeitando-se o prazo de 3 (três) dias úteis, a contar da data de ciência pelo MPRJ que o incidente afetou dados pessoais.

§ 3º - A comunicação deverá conter as informações exigidas no art. 48, § 1º, da Lei nº 13.709/2018 e na Resolução CD/ANPD nº 15/2024, sendo realizada através de formulário eletrônico disponibilizado pela ANPD, incluindo:

I - identificação e dados de contato do Ministério Público do Estado do Rio de Janeiro, enquanto entidade controladora, e do Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP);

II - os dados do encarregado ou de quem represente o controlador;

III - indicação se a notificação é completa ou parcial e, em caso de comunicação parcial, indicar se o caso versa sobre uma comunicação preliminar ou uma comunicação complementar;

IV - data e hora da detecção do incidente;

V - data e hora do incidente e sua duração, quando possível determiná-las;

VI - circunstâncias em que ocorreu a violação de segurança de dados pessoais, tais como: perda, roubo, cópia e vazamento;

VII - natureza e categoria dos dados pessoais afetados;

VIII - o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;

IX - resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento, além da sua natureza, isto é, se atingiu a confidencialidade, integridade ou disponibilidade dos dados;

X - os riscos relacionados ao incidente, com identificação das possíveis consequências e efeitos negativos sobre os titulares dos dados afetados;

XI - medidas de segurança, técnicas e administrativas utilizadas para a proteção dos dados pessoais, adotadas em momento anterior ou posterior ao incidente;

XII - resumo das medidas implementadas até o momento para controlar os possíveis danos ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;

XIII - os motivos da demora, no caso de a comunicação não ter sido realizada dentro do prazo de 3 (três) dias úteis;

XIV - a identificação do operador dos dados pessoais afetados, quando aplicável;

XV - a descrição do incidente, incluindo a causa principal, caso seja possível identificá-la;

XVI - o total de titulares cujos dados são objeto das atividades de tratamento afetadas pelo incidente, quando possível; e

XVII - outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

§ 4º - Caso não seja possível fornecer todas as informações no momento da comunicação preliminar, informações adicionais poderão ser fornecidas posteriormente, no prazo de 20 (vinte) dias úteis, a contar da data da comunicação, sendo que, no momento da comunicação preliminar, deverá ser informado à ANPD se serão fornecidas mais informações posteriormente, bem como quais meios estão sendo utilizados para obtê-las, ressaltando-se que a ANPD também poderá requerer informações adicionais a qualquer momento.

Art. 11 - O Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP) comunicará aos titulares a ocorrência de incidente de segurança relacionado a dados pessoais que possa acarretar risco ou dano relevante aos direitos e liberdades individuais dos titulares afetados.

§ 1º - Quando da avaliação da relevância do risco ou dano, deverão ser considerados com maior peso as situações em que o incidente:

I - envolver dados sensíveis ou de pessoas em situação de vulnerabilidade, como crianças, adolescentes e idosos; e

II - tiver potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade.

§ 2º - Ainda no momento da avaliação da relevância do risco ou dano, deverá ser considerado o volume de dados envolvidos, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados.

§ 3º - A comunicação aos titulares deverá ser realizada no prazo de 3 (três) dias úteis, fazendo uso de linguagem simples e de fácil entendimento, e deverá indicar o seguinte:

I - a descrição da natureza e da categoria de dados pessoais afetados;

II - as medidas técnicas e de segurança utilizadas para a proteção dos dados;

III - os riscos relacionados ao incidente, com identificação dos possíveis impactos aos titulares, tais como se o titular de dados pessoais pode ser vítima de fraude em razão do incidente;

IV - os motivos da demora, no caso de a comunicação não ter sido feita no prazo de 3 (três) dias úteis;

V - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;

VI - a data do conhecimento do incidente de segurança; e

VII - onde o titular pode obter mais informações sobre o incidente e, quando aplicável, os dados de contato do encarregado.

§ 4º - A comunicação do incidente aos titulares de dados deverá ocorrer de forma direta e individualizada, caso seja possível identificá-los.

§ 5º - Se, pela natureza do incidente, não for possível identificar individualmente os titulares afetados, devem ser comunicados todos os presentes na base de dados comprometida.

§ 6º - Caso a comunicação direta e individualizada mostre-se inviável ou não seja possível identificar, parcial ou integralmente, os titulares afetados, deverá ser comunicada a ocorrência do incidente, no prazo e com as informações requeridas, pelos meios de divulgação disponíveis, tais como sítio eletrônico, aplicativos, mídias sociais e canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização, pelo período de, no mínimo, 3 (três) meses.

§ 7º - A depender da gravidade do incidente e do número de titulares afetados, o Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP) poderá recomendar a divulgação do fato no sítio eletrônico, nas redes sociais e em outros meios de comunicação oficiais do Ministério Público, bem como a articulação junto à Ouvidoria para informe à sociedade civil.

§ 8º - Poderá ser considerada boa prática, para os fins do disposto no art. 52, § 1º, IX, da LGPD, a inclusão, na comunicação ao titular, de recomendações aptas a reverter ou mitigar os efeitos do incidente.

Art. 12 - O Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP) elaborará documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio da responsabilização e da prestação de contas, observando-se o disposto no art. 6º, X, da LGPD, indicando a forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares, ou os motivos da ausência de comunicação, quando for o caso.

§ 1º - Deverá ser mantido o registro do incidente de segurança, inclusive daquele não comunicado à ANPD e aos titulares, pelo prazo mínimo de 5 (cinco) anos, contado a partir da data do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.

§ 2º - O registro do incidente deverá conter, no mínimo:

I - a data de conhecimento do incidente;

II - a descrição geral das circunstâncias em que o incidente ocorreu;

III - a natureza e a categoria de dados afetados;

IV - o número de titulares afetados;

V - a avaliação do risco e os possíveis danos aos titulares;

VI - as medidas de correção e mitigação dos efeitos do incidente, quando aplicável;

VII - a forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares; e

VIII - os motivos da ausência de comunicação, quando for o caso.

Art. 13 - Ao Encarregado pelo Tratamento de Dados Pessoais caberá a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), conforme o art. 7º, inciso X, da Resolução GPGJ nº 2.699/2025:

I - para o tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, observando-se as exceções previstas no art. 4º, inciso III, da LGPD;

II - quando houver infração à LGPD em decorrência do tratamento de dados pessoais por órgãos públicos, conforme dispõem os arts. 31 e 32 da LGPD, combinados;

III - a qualquer momento, sob determinação da ANPD, como preceitua o art. 38 da LGPD;

IV - a qualquer momento, sob determinação da UEPDAP, como preceitua o art. 137, VIII, da Resolução CNMP nº 281/2023;

V - quando constatar a possibilidade de ocorrer impacto na privacidade dos dados pessoais.

Capítulo III

Prevenção aos Incidentes com Dados Pessoais

Art. 14 - As seguintes diretrizes devem ser seguidas para prevenir a ocorrência de incidentes:

I - treinamentos e aculturamento em segurança da informação e proteção de dados para membros, servidores, alunos-residentes, estagiários e terceirizados do MPRJ;

II - criação de procedimentos operacionais para resposta padrão a incidentes com dados pessoais, orientados por um plano, os quais serão testados e validados regularmente;

III - adoção das melhores práticas e os meios técnicos adequados para a proteção dos dados pessoais, tais como *firewalls* e hierarquização de acessos;

IV - avaliação periódica de riscos relacionados a incidentes, criação de ambiente de testes e simulações de incidentes;

V - estabelecimento de rigoroso controle de acesso ao ambiente físico e digital do MPRJ, contemplando todos os sistemas e ferramentas aprovados.

Capítulo IV

Disposições Finais e Transitórias

Art. 15 - No prazo de 6 (seis) meses, a contar da publicação deste Plano, a Secretaria de Tecnologia da Informação e de Comunicação (STIC) elaborará protocolos técnicos específicos de prevenção e resposta a incidentes de segurança.

Art. 16 - Esta Resolução entra em vigor na data da sua publicação, ficando revogada a Resolução GPGJ nº 2.548, de 29 de agosto de 2023.

Rio de Janeiro, 29 de maio de 2025.

Antonio José Campos Moreira

Procurador-Geral de Justiça