

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 19/06/2026 | Edição: 113 | Seção: 1 | Página: 74

Órgão: Ministério da Gestão e da Inovação em Serviços Públicos/Fundação Escola Nacional de Administração Pública

RESOLUÇÃO ENAP Nº 96, DE 11 DE JUNHO DE 2026

Dispõe sobre o processo de comunicação de incidentes de segurança, dos pedidos de acesso à informação e da observância à Lei Geral de Proteção de Dados Pessoais (LGPD), e o registro de compartilhamento de dados pessoais com terceiros no âmbito da Fundação Escola Nacional de Administração Pública (Enap).

O CONSELHO DIRETOR DA FUNDAÇÃO ESCOLA NACIONAL DE ADMINISTRAÇÃO PÚBLICA - ENAP, no uso das atribuições que lhe confere o art. 17 do Estatuto da Fundação Escola Nacional de Administração Pública, aprovado pelo Decreto nº 10.369, de 22 de maio de 2020, e suas alterações, e em atendimento ao disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI), nos Enunciados nº 04, de 2022, e nº 12, de 2023, ambos da Controladoria-Geral da União - CGU, na Resolução CD/ANPD nº 15, de 24 de abril de 2024, e nas determinações do Acórdão nº 1372/2025-TCU-Plenário, e o constante dos autos do processo nº 04600.004114/2025-87, resolve:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Resolução estabelece os procedimentos internos para:

I - a comunicação de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares;

II - o tratamento dos pedidos de acesso à informação nos termos da Lei nº 12.527, de 18 de novembro de 2011, em harmonização com a Lei nº 13.709, de 14 de agosto de 2018; e

III - o mapeamento e o registro do compartilhamento de dados pessoais com terceiros.

Art. 2º Considera-se incidente de segurança qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais.

§ 1º O incidente de segurança que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, nos casos em que:

I - a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço; ou

II - ocasionar danos materiais ou morais aos titulares, tais como:

a) discriminação;

b) violação à integridade física, ao direito à imagem e à reputação;

c) fraudes financeiras; ou

d) roubo de identidade.

§ 2º Considera-se incidente com dados em larga escala aquele que abranger número significativo de titulares, considerando:

I - o volume de dados envolvidos;

II - a duração;

III - a frequência; e



IV - a extensão geográfica da localização dos titulares.

CAPÍTULO II

da COMUNICAÇÃO DE INCIDENTES de segurança

Art. 3º Qualquer servidor efetivo ou comissionado que tomar conhecimento de incidente de segurança deverá comunicar imediatamente o fato à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR/Enap).

Parágrafo único. A Coordenação-Geral de Tecnologia da Informação (CGTI), o Gestor de Segurança da Informação e a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR/Enap) deverão reportar o evento ao Encarregado pelo Tratamento de Dados Pessoais, para avaliação de riscos regulatórios, legais e aos titulares.

Art. 4º O Gestor de Segurança da Informação, o Comitê de Segurança da Informação e a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR/Enap) deverão comunicar formalmente ao Encarregado pelo Tratamento de Dados Pessoais toda ocorrência de incidente cibernético que:

I - envolva, direta ou indiretamente, dados pessoais; ou

II - apresente indícios de risco à confidencialidade, à integridade, à disponibilidade ou à autenticidade de dados pessoais.

Parágrafo único. A inexistência de confirmação imediata quanto à exposição de dados pessoais não afasta o dever de comunicação preventiva ao Encarregado.

Art. 5º Compete à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR/Enap):

I - manter o Encarregado pelo Tratamento de Dados Pessoais permanentemente informado sobre a evolução do incidente;

II - fornecer os subsídios técnicos necessários à avaliação de risco ou de dano relevante aos titulares de dados pessoais; e

III - apoiar o Encarregado na elaboração das comunicações à Agência Nacional de Proteção de Dados (ANPD) e aos titulares, quando aplicável.

Art. 6º Compete ao Comitê de Segurança da Informação:

I - acompanhar, de forma executiva, os incidentes cibernéticos que envolvam dados pessoais;

II - assegurar a articulação entre a governança de segurança da informação e a proteção de dados pessoais; e

III - deliberar sobre medidas estruturais de prevenção e mitigação, sempre que o incidente evidenciar fragilidades sistêmicas.

Art. 7º O Encarregado deverá comunicar à Agência Nacional de Proteção de Dados e ao titular a ocorrência de incidente que possa acarretar risco ou dano relevante.

Parágrafo único. A comunicação à Agência Nacional de Proteção de Dados seguirá os requisitos de conteúdo previstos no art. 9º, § 2º, desta Resolução.

Art. 8º Considera-se que um incidente de segurança pode acarretar risco ou dano relevante aos dados pessoais dos titulares quando puder afetar significativamente seus interesses e direitos fundamentais e, cumulativamente, envolver pelo menos um dos seguintes critérios:

I - dados pessoais sensíveis;

II - dados de crianças, adolescentes ou 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.



Art. 9º A comunicação de incidente de segurança à Agência Nacional de Proteção de Dados deverá ser realizada por meio do Encarregado pelo Tratamento de Dados Pessoais no prazo de três dias úteis, ressalvada a existência de prazo diverso previsto em legislação específica.

§ 1º O prazo previsto no caput conta-se da ciência, pelo Encarregado, de que o incidente envolveu dados pessoais.

§ 2º A comunicação de incidente de segurança deverá conter as seguintes informações:

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

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

III - as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente, com identificação dos possíveis impactos aos titulares;

V - os motivos da demora, no caso de a comunicação não ter sido realizada no prazo previsto no caput deste artigo;

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;

VII - a data da ocorrência do incidente, quando possível determiná-la, e a de seu conhecimento pelo Encarregado pelo Tratamento de Dados Pessoais;

VIII - os dados do Encarregado pelo Tratamento de Dados Pessoais;

IX - a identificação da Fundação Escola Nacional de Administração Pública;

X - a identificação do operador, quando aplicável;

XI - descrição sucinta do incidente, incluída a causa principal, se identificada; e

XII - o total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.



Art. 10. A comunicação de incidente de segurança ao titular deverá ser realizada por meio do Encarregado pelo Tratamento de Dados Pessoais no prazo de três dias úteis contados do conhecimento do Encarregado de que o incidente afetou dados pessoais, e deverá conter as seguintes informações:

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, observados os segredos comercial e industrial;

III - os riscos relacionados ao incidente, com identificação dos possíveis impactos aos titulares;

IV - os motivos da demora, no caso de a comunicação não ter sido feita no prazo do caput deste artigo;

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;

VII - o contato para obtenção de informações e, quando aplicável, os dados de contato do Encarregado pelo Tratamento de Dados Pessoais;

VIII - sistemas, serviços ou ativos afetados;

IX - estimativa inicial de impacto sobre dados pessoais; e

X - responsável técnico pelo acompanhamento do incidente;

§ 1º A comunicação do incidente aos titulares de dados deverá atender aos seguintes critérios:

I - fazer uso de linguagem simples e de fácil entendimento; e

II - ocorrer de forma direta e individualizada, caso seja possível identificá-los.

§ 2º Considera-se comunicação de forma direta e individualizada aquela realizada pelos meios usualmente utilizados pela Enap para contatar o titular, tais como telefone, e-mail ou mensagem eletrônica.

§ 3º Caso a comunicação direta e individualizada mostre-se inviável ou não seja possível identificar, parcial ou integralmente, os titulares afetados, o Encarregado pelo Tratamento de Dados Pessoais deverá comunicar a ocorrência do incidente, no prazo e com as informações definidas no caput, pelos meios de divulgação disponíveis, tais como seu sítio eletrônico, aplicativos, suas 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, três meses.

§ 4º O Encarregado pelo Tratamento de Dados Pessoais deverá juntar ao processo de comunicação de incidente uma declaração de que foi realizada a comunicação aos titulares, constando os meios de comunicação ou divulgação utilizados, em até três dias úteis, contados do término do prazo de que trata o caput deste artigo.

CAPÍTULO III

do REGISTRO DO INCIDENTE DE SEGURANÇA

Art. 11. O Encarregado pelo Tratamento de Dados Pessoais efetuará o registro do incidente de segurança, e a Enap deverá manter o referido registro, inclusive daquele não comunicado à Agência Nacional de Proteção de Dados e aos titulares, nas hipóteses previstas na Resolução CD/ANPD nº 15, de 24 de abril de 2024, pelo prazo mínimo de cinco anos, contado da data do registro, salvo obrigação legal que exija prazo superior.

Parágrafo único. 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 Agência Nacional de Proteção de Dados e aos titulares; e

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

Art. 12. Após a conclusão do tratamento do incidente de segurança, deverá ser elaborado relatório técnico contendo, no mínimo:

I - descrição detalhada do incidente;

II - análise das causas e das vulnerabilidades exploradas;

III - impactos identificados;

IV - medidas adotadas para contenção e mitigação; e

V - recomendações para prevenção de ocorrências semelhantes.

CAPÍTULO IV

dos pedidos de acesso à informação e da observância à lei geral de proteção de dados pessoais

Art. 13. A Ouvidoria da Enap, por meio do Serviço de Informação ao Cidadão - SIC, de que trata o inciso I do art. 9º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI), é a unidade responsável pelo recebimento, tratamento e fornecimento das respostas nos pedidos de acesso à informação.

Art. 14. Compete à Autoridade de Monitoramento da Lei de Acesso à Informação da Enap assegurar o cumprimento das normas de acesso à informação e orientar as unidades da Enap quanto à aplicação da Lei nº 12.527, de 18 de novembro de 2011, no tratamento e decisão dos pedidos de acesso à informação.



Art. 15. As decisões proferidas no âmbito dos pedidos de acesso à informação que tratem da publicidade ou da restrição de acesso a informações contendo dados de pessoas naturais deverão ser fundamentadas nos arts. 3º e 31 da LAI.

Parágrafo único. A Lei nº 13.709, de 14 de agosto de 2018, será aplicada de forma complementar e harmônica à LAI, sendo vedada sua invocação genérica ou abstrata como fundamento exclusivo para a negativa de acesso a informações de interesse público.

Art. 16. A análise dos pedidos de acesso à informação que envolvam dados pessoais deverá observar critérios objetivos, considerando, cumulativamente:

I - a observância da publicidade como preceito geral e do sigilo como exceção;

II - a garantia dos direitos fundamentais de acesso à informação e de proteção de dados pessoais;

III - o tratamento adequado dos dados pessoais, com respeito à intimidade, à vida privada, à honra e à imagem das pessoas, bem como às liberdades e garantias individuais, nos termos da Lei nº 13.709, de 14 de agosto de 2018;

IV - a necessidade, a adequação e a proporcionalidade da eventual restrição de acesso; e

V - a possibilidade de divulgação parcial da informação, mediante a adoção de técnica de ocultação, como o tarjamento, a anonimização ou a pseudonimização.

Art. 17. A presença de dados pessoais não ensejará negativa total de acesso à informação quando for possível o tratamento e a proteção do dado por meio da ocultação, assegurado o acesso à parte não sigilosa do documento.

§ 1º A ocultação do dado pessoal deverá ser adotada sempre que a proteção do dado for suficiente para resguardar os direitos da pessoa natural, sem prejuízo à compreensão do conteúdo informacional do documento.

§ 2º A negativa total de acesso à informação somente será admitida quando as técnicas de ocultação se mostrarem inviáveis ou insuficientes para a proteção das informações pessoais envolvidas.

Art. 18. A unidade técnica responsável pela produção ou custódia do documento deverá realizar a ocultação das informações protegidas, quando cabível.

Parágrafo único. Em caso de dúvida quanto à possibilidade ou à extensão da restrição de acesso, a Autoridade de Monitoramento da Lei de Acesso à Informação, em conjunto com o Encarregado pelo Tratamento de Dados Pessoais, poderá ser acionada para a análise da demanda, observando os limites do art. 31 da Lei nº 12.527, de 18 de novembro de 2011, em consonância com as cautelas e premissas balizadoras da Lei nº 13.709, de 14 de agosto de 2018.

Art. 19. A ocultação das informações deverá ser realizada por meio de ferramenta ou software que impeça a reversão do conteúdo originalmente ocultado.

Art. 20. Toda negativa de acesso total ou parcial à informação, fundamentada na proteção de dados pessoais, deverá ser devidamente motivada e acompanhada de justificativa detalhada, expedida pela área competente, indicando, no mínimo:

I - os dados ou informações objeto de restrição de acesso;

II - de que forma a divulgação da informação afrontaria as disposições legais aplicáveis à proteção de dados pessoais; e

III - as medidas de ocultação avaliadas ou adotadas, quando cabíveis.

Art. 21. A Enap publicará, anualmente, em seu sítio eletrônico oficial, relatório consolidado contendo estatísticas sobre as negativas de acesso à informação fundamentadas na proteção de dados pessoais, indicando, no mínimo:

I - o quantitativo total de negativas parciais e totais realizadas no período;

II - o rol das razões e dos fundamentos legais mais frequentemente utilizados nas justificativas;

e



III - as medidas adotadas pela Fundação para ampliar o acesso à informação, em conformidade com o princípio da transparência pública.

CAPÍTULO V

do registro do COMPARTILHAMENTO de dados pessoais

Art. 22. O compartilhamento de dados pessoais com terceiros deverá observar:

I - a finalidade específica do tratamento;

II - a base legal aplicável;

III - a formalização do compartilhamento por instrumento jurídico ou administrativo adequado; e

IV - a observância das disposições da Lei nº 13.709, de 14 de agosto de 2018, e do Decreto nº 10.046, de 9 de outubro de 2019.

Art. 23. A Enap manterá registro atualizado de todos os compartilhamentos de dados pessoais com entidades externas, públicas ou privadas.

§ 1º As unidades administrativas deverão informar ao Encarregado a finalidade do compartilhamento e a base legal utilizada.

§ 2º O registro dos compartilhamentos e dos fluxos de dados deverá ser mantido pelo prazo mínimo de cinco anos.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 24. Os casos omissos ou as dúvidas na aplicação desta Resolução serão triados pelo Encarregado pelo Tratamento de Dados Pessoais, a quem competirá decidir, ouvida, se necessário, a Diretoria-Executiva, a Procuradoria Jurídica e a Ouvidoria da Enap.

§ 1º A decisão do Encarregado será submetida ao Conselho Diretor por meio de nota técnica que contenha o relato do caso e as motivações da decisão tomada, para ciência e ratificação, no prazo máximo de trinta dias, quando a situação tratada extrapole situações individuais ou causem impacto institucional, a critério do Encarregado ou a pedido de membro do Conselho Diretor.

§ 2º Quando o Conselho Diretor entender necessário, poderá solicitar suporte técnico de qualquer órgão da Enap ou de consultor externo, que apresentarão manifestações técnicas aptas a subsidiar sua decisão.

Art. 25. Esta Resolução entra em vigor no primeiro dia útil do mês subsequente à sua publicação.

BETÂNIA LEMOS

Este conteúdo não substitui o publicado na versão certificada.

