



MINISTÉRIO DAS COMUNICAÇÕES
Secretaria-Executiva do Ministério das Comunicações
Subsecretaria de Tecnologia da Informação
RESOLUÇÃO Nº 42/2026/MCOM

Brasília, 07 de abril de 2026.

Aprova a Norma Complementar para a Utilização Segura de Soluções de Computação em Nuvem .

O SUBCOMITÊ DE SEGURANÇA DA INFORMAÇÃO instituído pela Portaria nº 20.054, de 10 de outubro de 2025, representado pelo Gestor de Segurança da Informação, designado por meio da Portaria MCOM nº 308, de 13 de agosto de 2024, no uso das atribuições que lhe confere o artigo 17, da Resolução nº 26/2024/MCOM, resolve:

Art. 1º Aprovar a Norma Complementar para a Utilização Segura de Soluções de Computação em Nuvem.

Art. 2º Fica revogada a Portaria MCOM nº 5.053, de 24 de março de 2022.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

GUSTAVO HENRIQUE DE SOUTO SILVA
Gestor de Segurança da Informação
Presidente do Subcomitê de Segurança da Informação

**NORMA COMPLEMENTAR PARA A UTILIZAÇÃO SEGURA DE SOLUÇÕES DE
COMPUTAÇÃO EM NUVEM**

1. DISPOSIÇÕES GERAIS

Art. 1º Esta Norma Complementar estabelece diretrizes gerais para a utilização segura de soluções de computação em nuvem no âmbito do Ministério das Comunicações, em consonância com a legislação federal, os normativos superiores e as boas práticas reconhecidas de segurança da informação, proteção de dados pessoais e governança digital.

Art. 2º A aplicação desta Norma Complementar deverá ocorrer de forma integrada aos demais instrumentos normativos vigentes, não substituindo nem restringindo as competências, responsabilidades ou procedimentos estabelecidos em normas específicas.

Parágrafo único. Na hipótese de divergência interpretativa, deverão prevalecer os normativos hierarquicamente superiores.

Art. 3º Para fins desta Norma Complementar, aplicam-se os conceitos definidos nos normativos federais vigentes sobre segurança da informação, proteção de dados pessoais, computação em nuvem e governança digital.

2. PRINCÍPIOS E DIRETRIZES GERAIS

Art. 4º A utilização de soluções de computação em nuvem deverá observar, no mínimo, os seguintes princípios:

- I – legalidade e conformidade normativa;
- II – segurança da informação baseada em risco;
- III – proteção de dados pessoais e da privacidade;
- IV – responsabilidade e rastreabilidade;
- V – transparência e auditabilidade;
- VI – continuidade dos serviços; e
- VII – proporcionalidade entre riscos, controles e custos.

Art. 5º As decisões relacionadas à adoção, migração ou manutenção de serviços em computação em nuvem deverão considerar o interesse público, a criticidade dos serviços institucionais e os impactos operacionais, jurídicos e reputacionais associados.

3. PROTEÇÃO DE DADOS PESSOAIS E PRIVACIDADE

Art. 6º O tratamento de dados pessoais em soluções de computação em nuvem deverá observar os princípios e requisitos previstos na legislação de proteção de dados pessoais, bem como as diretrizes institucionais correlatas.

Art. 7º Deverão ser considerados, de forma geral, princípios de proteção de dados desde a concepção e por padrão (privacy by design e privacy by default), de modo compatível com os normativos aplicáveis.

Art. 8º As soluções de computação em nuvem deverão permitir a adoção de medidas proporcionais de segurança e governança que contribuam para a prevenção de incidentes e para a mitigação de riscos à privacidade e aos direitos dos titulares.

4. SEGURANÇA DA INFORMAÇÃO EM AMBIENTES DE NUVEM

Art. 9º A utilização de ambientes de computação em nuvem deverá observar uma abordagem de segurança da informação orientada por risco, compatível com a criticidade das informações e dos serviços institucionais.

Art. 10 As arquiteturas tecnológicas adotadas deverão considerar práticas reconhecidas de segurança, incluindo, quando pertinente, modelos de controle de acesso, segregação lógica, proteção criptográfica e monitoramento.

Parágrafo único. A definição das soluções técnicas observará as diretrizes e competências estabelecidas nos normativos específicos aplicáveis.

Art. 11 Os ambientes de computação em nuvem deverão permitir a rastreabilidade de acessos, operações e eventos relevantes, respeitados os limites e responsabilidades definidos em normativos próprios.

5. GOVERNANÇA, MONITORAMENTO E CONFORMIDADE

Art. 12 O uso de soluções de computação em nuvem deverá estar inserido no modelo de governança institucional, observando as estruturas, papéis e instâncias decisórias definidas pelo Ministério.

Art. 13 Deverão ser adotados mecanismos adequados de acompanhamento e verificação da conformidade dos ambientes de computação em nuvem com os requisitos normativos aplicáveis.

Parágrafo único. Poderão ser utilizados, quando cabível, recursos de automação, monitoramento contínuo ou avaliação periódica, conforme diretrizes institucionais.

Art. 14 Os resultados das atividades de acompanhamento e avaliação poderão subsidiar decisões relacionadas à continuidade, à adequação ou à revisão do uso das soluções de computação em nuvem.

6. ARQUITETURAS DISTRIBUÍDAS E CONTINUIDADE

Art. 15 A utilização de arquiteturas híbridas, distribuídas ou que envolvam múltiplos ambientes de computação em nuvem deverá observar os requisitos de segurança da informação, proteção de dados pessoais e continuidade dos serviços.

Art. 16 Na adoção de soluções de computação em nuvem deverão ser considerados aspectos relacionados à continuidade operacional, à recuperação de serviços e à resiliência, de forma compatível com os normativos vigentes.

7. INTELIGÊNCIA ARTIFICIAL EM AMBIENTES DE NUVEM

Art. 17 O uso de recursos de Inteligência Artificial em ambientes de computação em nuvem deverá observar diretrizes gerais de governança, ética, segurança e transparência, compatíveis com a legislação e os normativos aplicáveis.

Art. 18 A adoção de soluções que utilizem Inteligência Artificial deverá considerar os riscos associados ao tratamento de dados, ao impacto sobre processos institucionais e aos potenciais efeitos sobre direitos de terceiros.

Parágrafo único. Poderão ser considerados controles adicionais, conforme a criticidade e o contexto de uso da solução.

8. CONTRATAÇÕES E RELACIONAMENTO COM PROVEDORES

Art. 19 Os instrumentos contratuais relacionados a soluções de computação em nuvem deverão estar alinhados às diretrizes desta Norma Complementar e aos normativos aplicáveis.

Art. 20 Na contratação de serviços em computação em nuvem deverão ser considerados aspectos relacionados à segurança da informação, proteção de dados pessoais, continuidade, transparência e responsabilização, conforme previsto na legislação e nos normativos vigentes.

9. DAS RESPONSABILIDADES

Art. 21 As responsabilidades relacionadas à utilização de soluções de computação em nuvem no âmbito do Ministério das Comunicações observarão as competências estabelecidas nos normativos vigentes, cabendo às unidades envolvidas atuar de forma coordenada e complementar.

Art. 22 – Da Área de Tecnologia da Informação

Compete à área de Tecnologia da Informação, observadas as competências definidas em normativos específicos:

I – apoiar tecnicamente as unidades demandantes na adoção de soluções de computação em nuvem;

II – zelar pela aderência das soluções adotadas às diretrizes institucionais e normativas aplicáveis;

III – promover a articulação com provedores de serviços de computação em nuvem, quando cabível;

IV – contribuir para a implementação de mecanismos de segurança, monitoramento e continuidade, conforme diretrizes vigentes.

Art. 23 – Dos Gestores da Informação

Compete aos Gestores da Informação:

I – zelar pelo uso adequado das informações sob sua responsabilidade em ambientes de computação em nuvem;

II – observar as diretrizes de segurança da informação e proteção de dados pessoais aplicáveis;

III – participar das decisões relacionadas à adoção, manutenção ou descontinuidade de serviços em nuvem que envolvam informações sob sua gestão.

Art. 24 – Da Área de Segurança da Informação

Compete à área responsável pela Segurança da Informação:

I – orientar e acompanhar a aplicação das diretrizes de segurança da informação relacionadas ao uso de computação em nuvem;

II – apoiar a identificação e a análise de riscos relacionados aos ambientes de nuvem;

III – articular-se com as unidades competentes em caso de incidentes de segurança da informação, conforme normativos específicos.

Art. 25 – Das Unidades Usuárias

Compete às unidades usuárias de soluções de computação em nuvem:

I – utilizar os serviços em conformidade com esta Norma Complementar e com os normativos aplicáveis;

II – comunicar às instâncias competentes eventuais riscos, incidentes ou inconformidades identificadas;

III – colaborar com as ações de governança, segurança e conformidade relacionadas ao uso da nuvem.

Art. 26 – Dos Provedores de Serviço de Nuvem

Os provedores de serviços de computação em nuvem deverão observar as obrigações contratuais assumidas e as diretrizes estabelecidas na legislação e nos normativos aplicáveis, especialmente aquelas relacionadas à segurança da informação, à proteção de dados pessoais e à continuidade dos serviços.

10. DISPOSIÇÕES FINAIS

Art. 27 Os aspectos operacionais necessários à implementação das diretrizes desta Norma Complementar poderão ser detalhados em instrumentos complementares, observadas as competências institucionais e a legislação vigente.

Art. 28 Esta Norma Complementar deverá ser revisada periodicamente ou sempre que alterações relevantes no arcabouço normativo, tecnológico ou institucional assim o exigirem.



Documento assinado eletronicamente por **Gustavo Henrique de Souto Silva**, Subsecretário de **Tecnologia da Informação**, em 09/04/2026, às 18:51, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site <https://sei.mcom.gov.br/sei/verifica>, informando o código verificador **13247179** e o código CRC **AAF2F2B1**.

Anexos

Não Possui.