MINISTÉRIO DAS COMUNICAÇÕES
Secretaria-Executiva do Ministério das Comunicações
Subsecretaria de Tecnologia da Informação

RESOLUÇÃO MCOM Nº 46, DE 27 DE JULHO DE 2026

Aprova a Norma Complementar para a Cópia de Segurança e a Restauração de Dados.

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 Cópia de Segurança e a Restauração de Dados.

Art. 2º Fica revogada a Portaria MCOM nº 4.547/2021 de 28 de janeiro de 2021.

Art. 3° 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 CÓPIA DE SEGURANÇA E A RESTAURAÇÃO DE DADOS

1. DISPOSIÇÕES GERAIS

Art. 1º Esta Norma Complementar estabelece diretrizes, responsabilidades e requisitos mínimos para a realização de cópias de segurança, retenção e restauração de dados no âmbito do Ministério das Comunicações – MCOM.

Art. 2º Esta Norma aplica-se a todos os ativos de informação, sistemas, bases de dados e serviços sob responsabilidade do MCOM, independentemente do ambiente tecnológico em que estejam hospedados.

Art. 3º Esta Norma Complementar deve ser aplicada de forma integrada às demais normas complementares da Política de Segurança da Informação do MCOM, não devendo sobrepor, duplicar ou substituir requisitos nelas estabelecidos.

§1º Os controles relacionados à gestão de riscos, controle de acesso, inventário de ativos, continuidade de negócios, tratamento de incidentes, computação em nuvem e demais temas correlatos devem observar as respectivas normas complementares específicas.

§2º Esta Norma estabelece exclusivamente diretrizes e requisitos relacionados à cópia de segurança, retenção e restauração de dados.

2. DEFINIÇÕES

Art. 4º Para fins desta Norma, considera-se:

I – Cópia de Segurança (Backup): processo de criação de cópias de dados com o objetivo de permitir sua recuperação em caso de perda, corrupção ou indisponibilidade;

II – Restauração (Restore): processo de recuperação de dados a partir de cópias de segurança;

III – RPO (Recovery Point Objective): ponto máximo aceitável de perda de dados;

IV – RTO (Recovery Time Objective): tempo máximo aceitável para recuperação de serviços;

V – Dados de Recuperação: dados armazenados para fins de restauração, incluindo backups, snapshots e replicações;

VI – Instância Isolada de Recuperação: ambiente segregado, lógico ou físico, destinado ao armazenamento seguro de cópias de segurança;

VII – Ativo Crítico: item de configuração, lógico ou físico, essencial à continuidade dos serviços institucionais, cuja indisponibilidade gere impacto inaceitável à organização;

VIII – Componentes Tecnológicos Associados à Inteligência Artificial: bases de treinamento, modelos, parâmetros, códigos, configurações e demais artefatos necessários à operação, manutenção ou recuperação de soluções baseadas em Inteligência Artificial.

3. DIRETRIZES GERAIS

Art. 5º A cópia de segurança deve ser implementada como mecanismo essencial de proteção da informação e de suporte à recuperação de dados.

Art. 6º Os processos de backup e restauração devem ser definidos com base:

I – na criticidade do ativo de informação;

II – na classificação da informação;

III – nos requisitos legais, regulatórios e contratuais;

IV – nos impactos ao negócio;

V – nos objetivos de recuperação (RPO e RTO).

4. PROTEÇÃO DE DADOS PESSOAIS

Art. 7º Os processos de cópia de segurança e restauração de dados que envolvam dados pessoais devem observar os princípios e obrigações estabelecidos na legislação de proteção de dados pessoais.

§1º A retenção de cópias de segurança deve considerar os princípios da finalidade, necessidade e minimização, de forma a evitar a manutenção indevida de dados pessoais.

§2º A restauração de dados deve assegurar a manutenção da conformidade com as bases legais aplicáveis, devendo ser evitada a reintrodução indevida de dados pessoais que tenham sido eliminados ou anonimizados.

§3º O tratamento de dados pessoais nos processos de backup e restauração deve observar as normas institucionais de privacidade e proteção de dados do MCOM.

§4º Sempre que aplicável, devem ser adotadas medidas técnicas e administrativas para proteção dos dados pessoais armazenados em cópias de segurança, incluindo controle de acesso, rastreabilidade e mecanismos de proteção contra acesso não autorizado.

§5º A definição dos prazos de retenção, os procedimentos de descarte e as estratégias de restauração de cópias de segurança que envolvam dados pessoais devem contar com a participação ou validação do Encarregado pelo Tratamento de Dados Pessoais.

5. REQUISITOS DE CÓPIA DE SEGURANÇA

Art. 8º Devem ser realizadas cópias de segurança de:

I – dados operacionais e institucionais;

II – bases de dados;

III – arquivos e documentos digitais;

IV – códigos-fonte e artefatos de desenvolvimento;

V – configurações de sistemas e infraestrutura;

VI – registros necessários à reconstrução de ambientes;

VII – componentes tecnológicos associados a soluções de Inteligência Artificial, incluindo bases de treinamento, modelos, parâmetros, códigos, configurações e artefatos necessários à sua recuperação.

Art. 9º As cópias de segurança devem:

I – ser executadas de forma automatizada sempre que possível;

II – possuir periodicidade compatível com a criticidade do ativo;

III – garantir integridade, disponibilidade e confiabilidade dos dados;

IV – ser monitoradas quanto à sua execução e sucesso.

Art. 10. Deve existir, no mínimo:

I – uma cópia de recuperação armazenada de forma segregada do ambiente de produção;

II – para ativos críticos, mecanismo adicional de proteção contra exclusão, alteração indevida ou comprometimento das cópias de segurança, preferencialmente por meio de armazenamento imutável, offline ou logicamente segregado.

§1º Recomenda-se que a arquitetura de backup adote mecanismos de redundância e segregação compatíveis com as melhores práticas de mercado, incluindo estratégias de múltiplas cópias, múltiplos meios de armazenamento e armazenamento externo ou segregado.

§2º A definição da arquitetura de backup deverá considerar os riscos associados ao ativo protegido, sua criticidade e os objetivos de recuperação estabelecidos.

Art. 11. Os dados de backup devem ser protegidos contra acesso não autorizado, alteração indevida e exclusão acidental ou maliciosa.

Parágrafo único. O controle de acesso aos dados de backup deve observar a Norma Complementar para Controle de Acesso Lógico do MCOM.

6. RETENÇÃO E ARMAZENAMENTO

Art. 12. Os prazos de retenção das cópias de segurança devem considerar:

I – requisitos legais e regulatórios;

II – necessidades de negócio;

III – classificação da informação;

IV – diretrizes de gestão documental.

Parágrafo único. Recomenda-se que os processos de retenção, restauração e eliminação de cópias de segurança contendo dados pessoais observem os arts. 15 e 16 da Lei nº 13.709, de 14 de agosto de 2018.

Art. 13. O armazenamento das cópias de segurança deve:

I – ser realizado em ambiente seguro e controlado;

II – garantir segregação do ambiente de produção;

III – utilizar mecanismos de proteção adequados, inclusive criptografia quando aplicável.

§1º A proteção dos dados de backup deve ser equivalente ou superior à dos dados originais.

§2º O uso de serviços em nuvem para armazenamento de backups deve observar a Norma Complementar para Utilização Segura de Soluções de Computação em Nuvem.

§3º Quando envolver dados pessoais, devem ser observados os requisitos de proteção previstos na legislação de proteção de dados pessoais e nas normas institucionais aplicáveis.

§4º O descarte das cópias de segurança, ao término do prazo de retenção estabelecido, deve ser realizado de forma segura e rastreável, em conformidade com as diretrizes de gestão documental e a legislação vigente de proteção de dados pessoais.

7. RESTAURAÇÃO DE DADOS

Art. 14. Deve ser garantida a capacidade de restauração dos dados a partir das cópias de segurança, observados os objetivos de recuperação definidos para cada ativo.

Art. 15. Os procedimentos de restauração devem:

I – estar documentados;

II – ser testados periodicamente;

III – assegurar a integridade e completude dos dados restaurados.

Art. 16. A restauração de dados em situações de incidente deve observar a Norma Complementar para Tratamento de Incidentes Cibernéticos.

8. TESTES E VALIDAÇÃO

Art. 17. Devem ser realizados testes periódicos de restauração para verificar a efetividade das cópias de segurança.

Art. 18. Os testes devem:

I – ocorrer, no mínimo, anualmente, ou com maior frequência para ativos críticos;

II – ser realizados após mudanças significativas em sistemas ou infraestrutura;

III – ser registrados e documentados.

§1º Os ativos classificados como críticos devem possuir periodicidade de testes compatível com os respectivos RPO e RTO definidos pela organização.

§2º Os resultados dos testes de restauração devem ser registrados e utilizados para o aprimoramento contínuo dos procedimentos de recuperação.

Art. 19. Devem ser definidos critérios de sucesso para os testes de restauração, considerando, sempre que aplicável:

I – atendimento aos objetivos de recuperação definidos;

II – integridade dos dados restaurados;

III – completude das informações recuperadas;

IV – tempo efetivo de recuperação;

V – efetividade dos procedimentos documentados.

9. RESPONSABILIDADES

Art. 20. Compete às unidades responsáveis por ativos de informação:

I – definir requisitos de backup conforme criticidade;

II – assegurar que os dados sob sua responsabilidade estejam protegidos;

III – solicitar restauração quando necessário.

Art. 21. Compete à área de tecnologia da informação:

I – implementar e operar os mecanismos de backup;

II – garantir a execução, monitoramento e registro das cópias;

III – assegurar a disponibilidade dos processos de restauração;

IV – manter documentação atualizada dos procedimentos.

Art. 22. Compete à área responsável pela Segurança da Informação:

I – orientar quanto às diretrizes e requisitos de segurança;

II – acompanhar a conformidade com esta Norma;

III – apoiar a definição de requisitos de proteção dos dados;

IV – apoiar a avaliação dos requisitos de recuperação relacionados à continuidade dos negócios e à proteção das informações críticas.

10. CONFORMIDADE E AUDITORIA

Art. 23. O cumprimento desta Norma deve ser monitorado e avaliado periodicamente.

Parágrafo único. As atividades de auditoria devem observar a Norma Complementar para Gestão e Auditoria de Conformidade em Segurança da Informação.

11. DISPOSIÇÕES FINAIS

Art. 24. Os casos omissos devem ser tratados pela área de Segurança da Informação, em conjunto com a área de Tecnologia da Informação.

Art. 25. Esta Norma deve ser revisada periodicamente ou sempre que houver mudanças relevantes:

I – no ambiente tecnológico;

II – na legislação aplicável;

III – na estrutura organizacional;

IV – nos requisitos de continuidade de negócios;

V – nos requisitos institucionais de segurança da informação e proteção de dados pessoais.

Art. 26. Esta Norma entra em vigor na data de sua publicação.

Documento assinado eletronicamente por **Gustavo Henrique de Souto Silva**, **Subsecretário de Tecnologia da Informação**, em 27/07/2026, às 19:34, 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 **13452686** e o código CRC **C5A00B7F**.
