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

RESOLUÇÃO MCOM Nº 48, DE 27 DE JULHO DE 2026

Aprova a Norma Complementar para a Gestão de Riscos de Segurança da Informação.

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 Gestão de Riscos de Segurança da Informação.

Art. 2º Fica revogada a Portaria MCOM nº 5983 de 20 de junho de 2022.

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 GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

1. DISPOSIÇÕES GERAIS

Art. 1º Esta Norma Complementar estabelece diretrizes específicas para a gestão de riscos de segurança da informação no âmbito do Ministério das Comunicações – MCOM.

Art. 2º A gestão de riscos de segurança da informação constitui desdobramento da Política de Gestão de Riscos e Controles Internos do Ministério das Comunicações, devendo observar seus princípios, diretrizes, metodologia e estrutura de governança.

§1º Os critérios de apetite a risco, níveis de risco, tratamento, monitoramento e reporte deverão seguir os parâmetros definidos na Política de Gestão de Riscos e Controles Internos do MCOM.

§2º Esta Norma estabelece diretrizes específicas para identificação, análise, avaliação, tratamento e monitoramento dos riscos relacionados à segurança da informação, sem prejuízo das disposições da política corporativa.

Art. 3º Esta Norma 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 processos definidos nas demais normas complementares deverão utilizar os critérios e parâmetros de risco estabelecidos na Política de Gestão de Riscos e Controles Internos do MCOM e nesta Norma.

§2º As demais normas complementares deverão observar os critérios institucionais de risco vigentes no MCOM.

2. DEFINIÇÕES COMPLEMENTARES

Art. 4º Para fins desta Norma, aplicam-se as definições constantes da Política de Gestão de Riscos e Controles Internos do MCOM e, complementarmente:

I – Risco de Segurança da Informação: risco relacionado à confidencialidade, integridade, disponibilidade, autenticidade ou rastreabilidade das informações e dos ativos que as suportam;

II – Risco Cibernético: risco decorrente da exploração de vulnerabilidades ou da materialização de ameaças em ambientes digitais;

III – Evento de Segurança: ocorrência identificada em sistema, serviço, processo ou ativo de informação que indique possível comprometimento da segurança da informação;

IV – Ativo Crítico de Informação: ativo cujo comprometimento, indisponibilidade ou degradação possa causar impacto significativo aos objetivos institucionais ou à prestação de serviços do Ministério;

V – Risco Residual: risco remanescente após a implementação de medidas de tratamento;

VI – Ameaça: causa potencial de incidente capaz de explorar vulnerabilidades e causar danos aos ativos de informação.

3. DIRETRIZES GERAIS

Art. 5º A gestão de riscos de segurança da informação deve ser contínua, baseada em risco e orientada à tomada de decisão.

Art. 6º A gestão de riscos de segurança da informação deve:

I – apoiar a governança e a tomada de decisão institucional;

II – estar integrada ao planejamento estratégico, tático e operacional;

III – considerar o cenário de ameaças cibernéticas;

IV – utilizar informações atualizadas e confiáveis;

V – promover a proteção dos ativos de informação;

VI – subsidiar a definição e priorização de controles de segurança da informação.

Art. 7º A gestão de riscos deve apoiar a implementação das demais normas complementares da Política de Segurança da Informação do MCOM.

Parágrafo único. Os riscos relacionados à indisponibilidade de serviços e ativos críticos devem ser considerados nos processos de continuidade de negócios e recuperação de serviços.

4. GOVERNANÇA DA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 8º A gestão de riscos de segurança da informação observará a estrutura de governança institucional do Ministério das Comunicações.

Art. 9º Compete às instâncias de governança:

I – ao nível estratégico, definir diretrizes, supervisionar e acompanhar riscos relevantes à organização;

II – ao nível tático, coordenar, consolidar e monitorar as atividades de gestão de riscos;

III – ao nível operacional, identificar, analisar, avaliar, tratar e monitorar riscos relacionados às suas atividades e ativos sob sua responsabilidade.

Art. 10. O processo de gestão de riscos de segurança da informação deve manter fluxo contínuo de comunicação entre as instâncias envolvidas.

5. PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 11. O processo de gestão de riscos de segurança da informação deverá seguir a metodologia institucional de gestão de riscos, observando os requisitos específicos de segurança da informação estabelecidos nesta Norma.

Art. 12. O processo deve ser contínuo e considerar, no mínimo:

I – identificação de riscos de segurança da informação;

II – análise e avaliação de riscos;

III – tratamento de riscos;

IV – monitoramento e comunicação.

Art. 13. A gestão de riscos deve ser revisada ou atualizada sempre que houver:

I – mudanças significativas em sistemas, processos ou ativos;

II – identificação de novas vulnerabilidades críticas;

III – ocorrência de incidentes relevantes;

IV – alterações no ambiente tecnológico ou regulatório;

V – identificação de novas ameaças relevantes.

6. PRIORIZAÇÃO E TRATAMENTO DE RISCOS

Art. 14. A priorização dos riscos deve observar os critérios institucionais de risco definidos pelo MCOM.

Art. 15. O tratamento dos riscos poderá considerar, conforme o caso:

I – evitar;

II – mitigar;

III – aceitar;

IV – transferir;

V – eliminar.

Art. 16. A aceitação de riscos deve ser formalmente aprovada pela autoridade competente, conforme a estrutura de governança institucional.

7. INTEGRAÇÃO COM AS DEMAIS NORMAS COMPLEMENTARES

Art. 17. A gestão de riscos de segurança da informação constitui elemento orientador dos processos estabelecidos nas demais normas complementares da Política de Segurança da Informação do MCOM.

Art. 18. A gestão de riscos deve ser utilizada como base para:

I – priorização de vulnerabilidades;

II – tratamento de incidentes cibernéticos;

III – definição e revisão de controles de acesso;

IV – planejamento de continuidade de negócios;

V – definição de requisitos de segurança em ambientes tecnológicos;

VI – definição de requisitos de proteção de dados pessoais.

8. PROTEÇÃO DE DADOS PESSOAIS

Art. 19. A gestão de riscos deve considerar os riscos relacionados à proteção de dados pessoais.

Parágrafo único. Devem ser priorizados os riscos que possam resultar em violação de dados pessoais, especialmente aqueles relacionados a dados pessoais sensíveis ou de elevado impacto aos

titulares.

9. AUTOMAÇÃO E INTELIGÊNCIA ARTIFICIAL

Art. 20. A identificação, análise e monitoramento de riscos poderão utilizar ferramentas automatizadas ou soluções baseadas em Inteligência Artificial, sem prejuízo da validação e supervisão humana dos resultados.

10. MONITORAMENTO E REPORTE

Art. 21. Os riscos de segurança da informação devem ser monitorados continuamente.

Art. 22. Devem ser monitorados, no mínimo:

I – riscos classificados como altos ou críticos;

II – riscos aceitos;

III – eficácia dos planos de tratamento;

IV – riscos residuais;

V – riscos relacionados a ativos críticos de informação.

Art. 23. Devem ser elaborados relatórios gerenciais contendo, no mínimo:

I – principais riscos identificados;

II – nível de risco;

III – status dos planos de tratamento;

IV – riscos residuais.

Art. 24. Os riscos relevantes devem ser reportados às instâncias de governança competentes, observados os critérios definidos na Política de Gestão de Riscos e Controles Internos do MCOM.

11. DISPOSIÇÕES FINAIS

Art. 25. Esta Norma deve ser revisada periodicamente ou sempre que houver mudanças relevantes no ambiente tecnológico, regulatório ou organizacional.

Art. 26. Os casos omissos serão dirimidos pela instância responsável pela Segurança da Informação, em conjunto com a instância responsável pela Gestão de Riscos.

Art. 27. 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 19:35, 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 **13452707** e o código CRC **26D3DF3C**.
