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

RESOLUÇÃO MCOM Nº 47, DE 27 DE JULHO DE 2026

Aprova a Norma Complementar para o Gerenciamento de Vulnerabilidades.

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 o Gerenciamento de Vulnerabilidades.

Art. 2º Fica revogada a Portaria MCOM nº 7475 de 11 de novembro 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 O GERENCIAMENTO DE VULNERABILIDADES

1. DISPOSIÇÕES GERAIS

Art. 1º Esta Norma Complementar estabelece diretrizes, responsabilidades e requisitos para o gerenciamento de vulnerabilidades no âmbito do Ministério das Comunicações – MCOM.

Art. 2º Esta Norma aplica-se a todos os ativos de informação, sistemas, serviços, aplicações, infraestruturas e ambientes tecnológicos sob responsabilidade do MCOM.

Art. 3º Esta Norma deverá ser aplicada de forma integrada às demais normas complementares da Política de Segurança da Informação do MCOM.

§1º Os controles relacionados à gestão de riscos, controle de acesso, inventário de ativos, continuidade de negócios, tratamento de incidentes, computação em nuvem, gestão de mudanças e gestão de logs deverão observar os respectivos normativos específicos.

§2º Esta Norma trata exclusivamente do processo de identificação, avaliação, priorização, tratamento e monitoramento de vulnerabilidades.

§3º A utilização de mecanismos de automação ou de Inteligência Artificial no processo de gerenciamento de vulnerabilidades não afasta a responsabilidade dos agentes envolvidos nem dispensa os controles de validação e supervisão definidos nesta Norma e em normativos específicos.

2. DEFINIÇÕES

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

I – Vulnerabilidade: fragilidade ou deficiência em ativo, sistema, processo ou controle que possa ser explorada para comprometer a confidencialidade, integridade ou disponibilidade da informação;

II – Gerenciamento de Vulnerabilidades: processo contínuo de identificação, análise, priorização, tratamento e monitoramento de vulnerabilidades;

III – Superfície de Ataque: conjunto de ativos, interfaces, serviços, sistemas e pontos de exposição passíveis de exploração por agentes maliciosos;

IV – Priorização Baseada em Risco: método de classificação de vulnerabilidades que considera, além da severidade técnica, fatores como criticidade do ativo, exposição, impacto ao negócio e probabilidade de exploração;

V – Exploit Conhecido: código, técnica ou método publicamente conhecido capaz de explorar determinada vulnerabilidade;

VI – Ativo Crítico: ativo de informação cuja indisponibilidade, comprometimento ou degradação possa causar impacto significativo às atividades institucionais ou à prestação de serviços;

VII – Sistema IA-assistido: sistema que utiliza técnicas de Inteligência Artificial ou Aprendizado de Máquina para apoiar atividades de detecção, análise, priorização ou tratamento de vulnerabilidades;

VIII – Sugestão IA: recomendação gerada por sistema IA-assistido relativa à identificação, priorização, mitigação ou correção de vulnerabilidades.

3. DIRETRIZES GERAIS

Art. 5º O gerenciamento de vulnerabilidades deverá ser contínuo, baseado em risco e orientado por inteligência de ameaças.

Art. 6º O processo deverá considerar, no mínimo:

I – criticidade do ativo;

II – classificação da informação;

III – exposição do ativo;

IV – existência de exploração ativa;

V – impacto ao negócio;

VI – requisitos legais e regulatórios.

Art. 7º O gerenciamento de vulnerabilidades deverá estar integrado aos processos de gestão de riscos e continuidade de negócios, observados os normativos específicos.

Parágrafo único. Quando utilizadas soluções baseadas em Inteligência Artificial, deverão ser observados os requisitos de governança, segurança, transparência e supervisão definidos em normativos específicos.

4. PROTEÇÃO DE DADOS PESSOAIS

Art. 8º O tratamento de vulnerabilidades que envolvam dados pessoais deverá observar a legislação de proteção de dados pessoais vigente.

§1º Devem ser adotadas medidas para prevenir vazamento ou exposição indevida de dados pessoais decorrentes de vulnerabilidades.

§2º A correção de vulnerabilidades deverá priorizar ativos que tratem dados pessoais sensíveis ou de elevado impacto institucional.

§3º Quando soluções de Inteligência Artificial forem utilizadas no tratamento de vulnerabilidades envolvendo dados pessoais, deverão ser observados os princípios da necessidade, minimização, adequação e segurança previstos na legislação aplicável.

5. PROCESSO DE GERENCIAMENTO DE VULNERABILIDADES

Art. 9º O processo de gerenciamento de vulnerabilidades deverá ser formalmente estabelecido, implementado, mantido e continuamente aprimorado.

Art. 10. O processo deverá contemplar, no mínimo:

I – identificação dos ativos no escopo;

II – detecção de vulnerabilidades;

III – análise e priorização;

IV – tratamento e correção;

V – monitoramento contínuo;

VI – comunicação e reporte.

Parágrafo único. Sempre que tecnicamente viável, o processo deverá promover integração entre ferramentas de varredura, inventário de ativos e gerenciamento de chamados, assegurando a rastreabilidade das ações executadas.

6. DETECÇÃO DE VULNERABILIDADES

Art. 11. A detecção de vulnerabilidades deverá ser realizada por meio de ferramentas automatizadas, testes manuais e outras técnicas apropriadas.

Art. 12. As varreduras deverão:

I – ser contínuas para ativos críticos;

II – ocorrer periodicamente para os demais ativos;

III – ser realizadas após mudanças relevantes.

Art. 13. O processo deverá abranger, sempre que aplicável:

I – redes e infraestrutura;

II – sistemas e aplicações;

III – ambientes em nuvem;

IV – interfaces de programação de aplicações;

V – identidades e controles de acesso.

Art. 14. O MCOM poderá disponibilizar canal para recebimento de relatos de vulnerabilidades encaminhados por terceiros, observadas as diretrizes de divulgação responsável e os procedimentos internos de tratamento.

7. ANÁLISE E PRIORIZAÇÃO

Art. 15. A priorização das vulnerabilidades deverá ser baseada em risco.

Art. 16. Deverão ser considerados, no mínimo:

I – severidade técnica;

II – criticidade do ativo;

III – exposição do ativo;

IV – disponibilidade de exploit;

V – impacto ao negócio.

Art. 17. A priorização poderá considerar classificações ou recomendações geradas por ferramentas automatizadas ou soluções baseadas em Inteligência Artificial, desde que os critérios utilizados sejam passíveis de auditoria e validação.

8. TRATAMENTO E CORREÇÃO

Art. 18. As vulnerabilidades deverão ser tratadas por meio de:

I – aplicação de correções ou atualizações;

II – ajustes de configuração;

III – medidas mitigatórias temporárias;

IV – substituição de ativos, quando necessário.

Art. 19. As correções deverão ser testadas antes da implantação, observadas as diretrizes da Norma Complementar para a Gestão de Mudanças.

Art. 20. A priorização das correções deverá observar os níveis de risco definidos institucionalmente.

Art. 21. Vulnerabilidades classificadas como críticas ou que possuam exploração ativa conhecida poderão ser tratadas por procedimento prioritário e simplificado, observadas as diretrizes da Norma Complementar para a Gestão de Mudanças.

9. EXCEÇÕES E ACEITAÇÃO DE RISCO

Art. 22. A não correção de vulnerabilidades deverá ser formalmente justificada e aprovada conforme o processo de gestão de riscos.

§1º As exceções deverão possuir prazo determinado e plano de ação.

§2º As exceções deverão ser revisadas periodicamente.

10. MONITORAMENTO E MÉTRICAS

Art. 23. O processo deverá ser monitorado por meio de indicadores de desempenho.

Art. 24. Deverão ser acompanhados, no mínimo:

I – tempo médio de correção;

II – quantidade de vulnerabilidades por nível de risco;

III – taxa de reincidência;

IV – cobertura de varredura;

V – percentual de vulnerabilidades identificadas por mecanismos automatizados.

11. REGISTROS E AUDITORIA

Art. 25. Os registros relacionados ao gerenciamento de vulnerabilidades deverão ser mantidos e protegidos.

Parágrafo único. A gestão de logs deverá observar a Norma Complementar específica.

12. TERCEIROS E COMPUTAÇÃO EM NUVEM

Art. 26. Os serviços prestados por terceiros deverão atender aos requisitos desta Norma.

§1º As responsabilidades deverão estar formalmente definidas em contrato.

§2º O uso de serviços em nuvem deverá observar a Norma Complementar específica.

13. RESPONSABILIDADES

Art. 27. Compete às áreas de negócio:

I – identificar os ativos sob sua responsabilidade;

II – apoiar a priorização das vulnerabilidades;

III – apoiar a implementação das medidas corretivas quando aplicável.

Art. 28. Compete à área de Tecnologia da Informação:

I – executar processos de detecção e correção;

II – manter ferramentas e controles técnicos;

III – monitorar indicadores operacionais do processo.

Art. 29. Compete à área responsável pela Segurança da Informação::

I – definir diretrizes;

II – acompanhar a conformidade;

III – apoiar a gestão de riscos;

IV – monitorar a efetividade do processo de gerenciamento de vulnerabilidades.

14. DISPOSIÇÕES FINAIS

Art. 30. Esta Norma deverá ser revisada periodicamente ou sempre que ocorrerem alterações relevantes no ambiente tecnológico, nos requisitos legais ou nos normativos institucionais.

Art. 31. Os casos omissos serão dirimidos pela área responsável pela Segurança da Informação, observadas as competências estabelecidas na Política de Segurança da Informação do MCOM.

Art. 32. 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 **13452698** e o código CRC **A6ED29E7**.

Referência: Processo nº 53115.016204/2023-36 Documento nº 13452698