



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

RESOLUÇÃO MCOM Nº 40, DE 15 DE JANEIRO DE 2026.

Aprova a Norma Complementar para Uso Seguro de Serviço de Acesso à Internet.

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 Uso Seguro de Acesso a Internet.

Art. 2º Fica revogada a Portaria MCOM n 5055, de 24 de Março de 2022.

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

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

**NORMA COMPLEMENTAR PARA USO SEGURO DE SERVIÇO DE ACESSO À
INTERNET**

DIPOSIÇÕES PRELIMINARES

Art. 1º Esta Norma estabelece diretrizes, controles e procedimentos para o uso seguro do serviço de acesso à internet no âmbito do Ministério das Comunicações – MCOM.

Art. 2º Esta Norma aplica-se a todos os agentes públicos, estagiários, empregados, contratados e demais usuários que utilizem os serviços de conectividade providos pelo MCOM.

Art. 3º Para fins desta Norma, serão adotados os conceitos constantes do Glossário de Segurança da Informação do GSI/PR.

Art. 4º A gestão de identidades digitais, perfis, credenciais, autenticação, VPN, certificados digitais e equipamentos autorizados será regida exclusivamente pela Norma Complementar para Controle de Acesso Lógico.

RESPONSABILIDADES

Art. 5º Compete às chefias:

- I – divulgar as diretrizes desta Norma aos servidores subordinados;
- II – autorizar acessos excepcionais à internet quando previstos nestas regras;
- III – responder solidariamente pelos acessos autorizados.

Art. 6º Compete aos usuários:

- I – utilizar a internet exclusivamente para fins institucionais, salvo exceções controladas;
- II – zelar pela segurança das informações que trafegarem na rede, conforme orientações e diretrizes estabelecidas pela CGTI;
- III – reportar incidentes ou acessos indevidos.

Art. 7º Compete à CGTI:

- I – prover, administrar e monitorar os serviços de acesso à internet;
- II – implementar filtros, mecanismos de segurança e bloqueios;
- III – registrar logs de conexão e navegação;
- IV – aplicar e manter atualizados os controles de proteção de dados;
- V – utilizar soluções de IA para detectar ameaças, bloqueios dinâmicos e classificação de conteúdo.

USO DO SERVIÇO DE ACESSO À INTERNET

Seção I – Uso Permitido

Art. 8º O uso da internet deverá priorizar atividades institucionais relacionadas às atribuições do MCOM, observadas as diretrizes da Política de Segurança da Informação – POSIN.

Art. 9º É permitido acesso a serviços bancários e mercantis para necessidades pessoais, desde que:

- I – em volume razoável;
- II – sem prejuízo ao desempenho laboral;
- III – sem impacto na segurança da informação.

Art. 10. A autorização de acesso a conteúdos pessoais além dos limites do art. 9º dependerá de:

- I – solicitação do usuário;
- II – autorização formal da chefia imediata registrada em sistema;
- III – registro mantido pela CGTI para auditoria.

Seção II – Serviços Restritos

Art. 11. A liberação de serviços de streaming não previamente autorizados dependerá de requisição formal de autoridade CCE/FCE 13.

Art. 12. O acesso a mídias sociais e aplicativos de compartilhamento de conteúdo ocorrerá preferencialmente pela rede sem fio, podendo ser limitado ou bloqueado na rede

cabeada a critério de autoridade CCE/FCE 13.

Art. 13. A CGTI poderá estabelecer perfis de acesso diferenciados para áreas com necessidades específicas de navegação.

AUDITORIA, MONITORAMENTO E INTELIGÊNCIA ARTIFICIAL - IA

Art. 14. Todo tráfego e acesso à internet poderá ser monitorado pela CGTI, observada a legislação de proteção de dados pessoais.

Art. 15. A CGTI deverá registrar logs de:

- I – origem e horário de conexão;
- II – categorias de acesso;
- III – eventos de bloqueio e tentativas de violação;
- IV – incidentes gerados por mecanismos de IA.

Art. 16. As soluções de IA utilizadas poderão:

- I – classificar conteúdo automaticamente;
- II – detectar padrões anômalos de tráfego;
- III – priorizar alertas;
- IV – ajustar dinamicamente regras de bloqueio.

DA PROTEÇÃO DE DADOS

Art. 17. Os registros de acesso e navegação deverão observar os princípios de:

- I – finalidade;
- II – necessidade;
- III – minimização;
- IV – segurança;
- V – proporcionalidade.

Art. 18. Os logs utilizados rotineiramente deverão ser pseudonimizados sempre que possível.

Art. 19. A reidentificação de dados pseudonimizados somente poderá ocorrer mediante autorização formal e motivada.

Art. 20. Incidentes envolvendo dados pessoais deverão ser analisados e, quando necessário, comunicados conforme a legislação sobre proteção de dados.

VEDAÇÕES

Art. 21. É proibido:

- I – acessar conteúdos ilegais, ofensivos ou impróprios;
- II – acessar páginas que coloquem em risco a segurança institucional;
- III – utilizar ferramentas de anonimização, proxy oculto ou VPN não autorizada pela CGTI;
- IV – acessar salas de bate-papo recreativas;

V – acessar jogos online;

VI – utilizar softwares P2P;

VII – divulgar informações confidenciais via plataformas não autorizadas;

VIII – tentar burlar ou desativar mecanismos de filtragem ou IA;

IX – armazenar arquivos institucionais em serviços de nuvem não autorizados;

X – utilizar a internet para fins recreativos durante o expediente.

SANÇÕES

Art. 22. O descumprimento desta Norma constitui incidente de segurança da informação.

Art. 23. Os infratores estarão sujeitos às sanções administrativas, civis e penais cabíveis.

DISPOSIÇÕES FINAIS

Art. 24. Os casos omissos serão analisados pela CGTI e submetidos ao Subcomitê de Segurança da Informação.

Art.25. Esta Norma poderá ser revisada periodicamente pela CGTI, ou sempre que houver evolução tecnológica, alteração regulatória ou necessidade operacional.



Documento assinado eletronicamente por **Gustavo Henrique de Souto Silva**, Subsecretário de Tecnologia da Informação, em 21/01/2026, às 11:07, 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 **13092393** e o código CRC **3F3B5551**.

Anexos

Não Possui.