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

RESOLUÇÃO MCOM Nº 39, DE 15 DE JANEIRO DE 2026.

Aprova a Norma Complementar para Controle de Acesso Lógico do Ministério das Comunicações.

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 Controle de Acesso Lógico.

Art. 2º Fica revogada a Portaria MCOM n 2.805, de 11 de Junho de 2021.

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 CONTROLE DE ACESSO LÓGICO

DIPOSIÇÕES PRELIMINARES

Art. 1º Esta Norma estabelece regras, diretrizes, responsabilidades e controles referentes ao credenciamento, autenticação, autorização, uso e revogação de acessos lógicos aos ativos de informação do Ministério das Comunicações – MCOM.

§1º Para efeitos desta Norma, consideram-se incluídos no escopo os serviços de diretório, domínio, identidade digital, autenticação e autorização utilizados para acesso a sistemas corporativos.

§2º Esta Norma abrange, ainda, o uso e a gestão de certificados digitais para autenticação, assinatura digital e demais mecanismos de segurança previstos na ICP-Brasil, bem como as regras para acesso remoto por meio de VPN, disciplinando sua concessão, uso, restrições e medidas de proteção associadas.

Art. 2º Esta Norma aplica-se a todos os agentes públicos e demais usuários autorizados a utilizar recursos computacionais, sistemas, serviços e redes corporativas do MCOM.

Art. 3º Para fins desta Norma, serão adotadas as definições constantes:

I – do Glossário de Segurança da Informação do GSI/PR;

II – das normas ISO/IEC 27000 e 27002;

III – da Lei nº 13.709/2018 (LGPD).

Art. 4º A criação, alteração, uso e revogação de contas, perfis e credenciais observarão, além desta Norma:

I – a Política de Segurança da Informação do MCOM;

II – a Norma Complementar para Uso Seguro do Serviço de Acesso à Internet;

III – a Norma Complementar de Gestão de Incidentes, quando aplicável.

DO CREDENCIAMENTO E DAS CREDENCIAIS

Art. 5º O credenciamento constitui o processo de criação ou habilitação de contas e perfis de acesso, mediante autorização formal da chefia imediata.

Art. 6º As credenciais serão:

I – pessoais e intransferíveis;

II – concedidas somente após ingresso, retorno ou formalização contratual;

III – utilizadas de forma única nos serviços de diretório, domínio e sistemas integrados;

IV – revogadas na data do desligamento, afastamento superior a 60 dias ou motivo que gere perda de necessidade de acesso.

Art. 7º O padrão de identificação do usuário será composto por:

I – <primeiro_nome>.<último_sobrenome>;

II – sendo admitidas outras combinações do nome completo quando necessário.

Art. 8º Todos os usuários deverão assinar o **Termo de Responsabilidade e Confidencialidade**, conforme modelo constante do Anexo I.

DA AUTENTICAÇÃO E DAS SENHAS

Art. 9º A autenticação poderá ser realizada por:

I – senha;

II – autenticação multifator – MFA;

III – certificado digital;

IV – métodos autorizados pela CGTI.

Art. 10. As senhas deverão:

I – possuir no mínimo oito caracteres, contendo letras e números;

II – não reutilizar as duas últimas senhas;

III – ter validade máxima de 180 dias;

IV – ser alteradas obrigatoriamente no primeiro acesso.

Art. 11. É vedado ao usuário:

I – compartilhar credenciais;

II – utilizar credenciais de terceiros;

III – permanecer conectado em mais de uma estação simultaneamente;

IV – armazenar senhas em locais não seguros.

DOS RECURSOS DE REDE E SISTEMAS

Art. 12. Apenas equipamentos homologados pela CGTI poderão acessar a rede corporativa.

Art. 13. Em caráter excepcional, equipamentos particulares poderão ser autorizados, desde que:

I – haja justificativa formal;

II – atendam aos requisitos técnicos definidos pela CGTI;

III – seja respeitado o princípio da necessidade.

Art. 14. É vedado utilizar a rede corporativa para instalar, executar ou manter softwares, dispositivos ou serviços não homologados pela CGTI.

DA GESTÃO DE PERFIS E PRIVILÉGIOS

Art. 15. A concessão de perfis observará:

I – o princípio da necessidade;

II – o princípio do menor privilégio;

III – segregação de funções.

Art. 16. A CGTI manterá inventário de:

I – contas privilegiadas;

II – contas de serviço;

III – perfis sensíveis.

Art. 17. Os gestores de sistemas deverão:

I – manter matriz de perfis permanentemente atualizada;

II – validar solicitações de acesso;

III – definir regras de segregação de funções;

IV – garantir registro de logs de autenticação e ações privilegiadas.

DOS CERTIFICADOS DIGITAIS PARA AUTENTICAÇÃO

Art. 18. Os certificados digitais utilizados no âmbito do MCOM destinam-se exclusivamente às atividades institucionais, devendo ser empregados para autenticação, assinatura digital, criptografia ou quaisquer outros mecanismos formais de garantia de integridade, autenticidade e não repúdio, conforme regulamentação vigente.

Art. 19. A emissão, renovação, revogação e controle de certificados digitais seguirão as diretrizes da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, bem como as políticas internas de segurança da informação e gestão de identidade digital do MCOM.

Art. 20. As solicitações de emissão, renovação e revogação de certificados digitais funcionais deverão ser realizadas exclusivamente por meio do aplicativo Sou.Gov, observados os procedimentos oficiais da plataforma.

Art. 21. Compete à Coordenação-Geral de Tecnologia da Informação e Comunicação – CGTI:

I – manter cadastro atualizado dos certificados digitais emitidos, vinculados ou autorizados para uso no MCOM;

II – gerir o ciclo de vida dos certificados institucionais, incluindo emissão, renovação, suspensão e revogação;

III – orientar e apoiar tecnicamente os usuários quanto ao uso seguro do certificado digital;

IV – manter mecanismos de auditoria e registro de eventos associados ao uso de certificados digitais;

V – garantir que chaves privadas estejam protegidas por meios criptográficos adequados, preferencialmente em módulos de hardware seguro (HSM) ou dispositivos equivalentes;

VI – assegurar acesso restrito e controlado aos componentes sensíveis de certificação.

Art. 22. O usuário titular do certificado digital é responsável por:

I – zelar pela guarda, sigilo e uso exclusivo da chave privada associada ao seu certificado;

II – comunicar imediatamente à CGTI qualquer suspeita de comprometimento, extravio ou uso indevido;

III – utilizar o certificado exclusivamente para atividades institucionais;

IV – não compartilhar PIN, senha, token, smartcard, arquivo PFX ou quaisquer mecanismos que permitam acesso ao certificado digital.

Art. 23. É vedado:

I – armazenar certificados digitais institucionais em nuvem pública ou serviço não homologado pela CGTI;

II – copiar, exportar, transportar ou reproduzir certificados institucionais sem autorização formal da CGTI;

III – utilizar certificados digitais pessoais para atividades institucionais sem aprovação da CGTI;

IV – utilizar certificados digitais institucionais em dispositivos pessoais não autorizados.

Art. 24. A CGTI deverá estabelecer mecanismos técnicos que garantam:

I – proteção criptográfica dos certificados e chaves privadas;

II – trilhas de auditoria associando o uso do certificado ao respectivo titular;

III – bloqueio imediato do certificado em caso de comprometimento, desligamento ou conclusão de vínculo funcional;

IV – armazenamento seguro dos registros de autenticação e assinatura digital pelo período mínimo necessário.

Art. 25. Para fins de conformidade com a legislação de proteção de dados pessoais:

I – os dados pessoais associados a certificados digitais deverão ser tratados com finalidade específica e proporcional ao uso previsto;

II – logs de autenticação e de assinatura digital deverão ser armazenados pelo período estritamente necessário para auditoria, conforme obrigações legais;

III – o acesso aos registros de uso de certificados será restrito e condicionado à justificativa formal.

Art. 26. A violação das diretrizes relativas ao uso de certificados digitais será considerada incidente de segurança da informação e poderá sujeitar o infrator às penalidades administrativas, civis e criminais cabíveis.

DO USO REMOTO E DA VPN

Art. 27. O serviço de VPN (Virtual Private Network) disponibilizado pelo MCOM destina-se a prover acesso remoto seguro à rede corporativa e aos sistemas internos, devendo ser utilizado exclusivamente para fins institucionais.

Art. 28. A concessão de acesso ao serviço de VPN é condicionada:

I – à assinatura prévia do Termo de Responsabilidade para Acesso Remoto/VPN, constante do Anexo II desta Norma;

II – ao atendimento, pelo dispositivo utilizado, dos critérios técnicos de segurança definidos pela CGTI;

III – à autorização formal da chefia imediata;

IV – ao registro do pedido em sistema oficial de chamados;

V – à concessão preferencialmente por prazo determinado.

Art. 29. Compete à Coordenação-Geral de Tecnologia da Informação e Comunicação – CGTI:

I – definir os critérios de segurança obrigatórios para dispositivos utilizados em acesso remoto;

II – disponibilizar o software cliente de VPN e orientar sua instalação e configuração;

III – monitorar as sessões de VPN e suspender acessos em caso de risco, anomalia ou impacto negativo à rede;

IV – garantir que a infraestrutura de VPN utilize protocolos robustos de criptografia e autenticação;

V – manter logs completos de conexões, falhas, encerramentos e bloqueios preventivos;

VI – assegurar identificação unívoca do usuário durante a sessão remota.

Art. 30. O usuário autorizado ao uso da VPN é responsável por:

I – assegurar que o acesso remoto não seja utilizado por terceiros;

II – utilizar exclusivamente o software oficial de VPN fornecido pela CGTI;

III – manter solução de antimalware atualizada;

IV – responder por incidentes de segurança decorrentes do uso do dispositivo;

V – garantir que o uso da conexão permaneça em conformidade com as diretrizes de segurança do MCOM.

Art. 31. É vedado:

I – acessar a VPN por meio de equipamentos de uso público, como cybercafés ou terminais compartilhados;

II – transferir ou compartilhar credenciais pessoais de acesso;

III – utilizar a VPN para atividades não institucionais ou em desacordo com políticas internas;

IV – utilizar redes públicas não seguras para estabelecer conexão com a VPN.

Art. 32. A CGTI deverá implementar mecanismos técnicos que assegurem:

I – a integridade e a confidencialidade do túnel de comunicação estabelecido;

II – a identificação individualizada do usuário;

III – o encerramento imediato de sessões que apresentem comportamento anômalo ou risco à infraestrutura;

IV – coleta e armazenamento de logs de VPN para fins de auditoria e investigação de incidentes, respeitada a legislação vigente.

Art. 33. A violação das diretrizes relativas ao uso da VPN será considerada incidente de segurança da informação e poderá sujeitar o infrator à suspensão do acesso remoto, sem prejuízo das penalidades administrativas, civis e criminais aplicáveis.

DA PROTEÇÃO DE DADOS

Art. 34. O tratamento dos registros de acesso, logs de autenticação, autorização, perfis, alterações de privilégios, registros de VPN, uso de certificados digitais e demais dados pessoais relacionados ao controle de acesso lógico deverá observar integralmente a legislação de proteção de dados pessoais e os princípios de:

I – finalidade;

II – necessidade;

III – adequação;

IV – minimização;

V – livre acesso;

VI – qualidade dos dados;

VII – segurança;

VIII – prevenção;

IX – responsabilização e prestação de contas.

Art. 35. Os logs e registros associados ao controle de acesso deverão ser:

I – mantidos sob confidencialidade e acessíveis apenas a pessoal formalmente autorizado;

II – protegidos por mecanismos técnicos que garantam integridade, inviolabilidade e rastreabilidade;

III – armazenados por prazos definidos em política interna de retenção;

IV – preferencialmente pseudonimizados, sempre que a identificação direta não for necessária.

Art. 36. A anonimização ou pseudonimização será aplicada sempre que possível, respeitados os requisitos operacionais de auditoria, investigação de incidentes, prevenção a fraudes e continuidade dos serviços.

Art. 37. A reidentificação de dados pseudonimizados somente será permitida:

I – mediante autorização formal e motivada;

II – para fins de auditoria, investigação de incidentes, apuração disciplinar ou cumprimento de determinação judicial;

III – pelo tempo estritamente necessário ao atendimento da finalidade específica.

Art. 38. A CGTI deverá manter política específica de retenção e descarte de logs, contemplando:

I – os prazos mínimos e máximos de armazenamento;

II – diferenciação por tipo de registro (autenticação, privilégio, certificado digital, VPN, alterações de perfil etc.);

III – critérios objetivos para descarte seguro, irrecuperável e rastreável;

IV – documentação dos processos de eliminação.

Art. 39. O acesso a logs e trilhas de auditoria será:

I – individualizado;

II – registrado para rastreabilidade;

III – restrito a profissionais com necessidade comprovada;

IV – periodicamente revisado pela CGTI.

Art. 40. A utilização de mecanismos de Inteligência Artificial (IA) relacionados ao controle de acesso lógico deverá ser precedida de:

I – análise de riscos específica;

II – avaliação de impacto à proteção de dados pessoais;

III – definição de controles de minimização e rastreabilidade;

IV – supervisão humana;

V – aprovação pela CGTI.

Art. 41. A CGTI deverá revisar anualmente os processos relativos ao tratamento de dados pessoais no controle de acesso lógico, incluindo:

I – retenção;

II – descarte;

III – segregação de funções;

IV – segurança técnica;

V – conformidade regulatória.

DAS RESPONSABILIDADES

Seção I – Da Coordenação-Geral de Tecnologia da Informação e Comunicação – CGTI

Art. 42. Compete à CGTI:

I – administrar os serviços de autenticação, diretórios, identidades digitais e trilhas de auditoria;

II – implementar e manter mecanismos de segurança, monitoramento e prevenção de incidentes;

III – revisar periodicamente perfis, privilégios e acessos concedidos;

IV – homologar equipamentos e soluções tecnológicas utilizadas para acesso lógico;

V – realizar bloqueios preventivos sempre que houver suspeita de comprometimento;

VI – apoiar processos de investigação disciplinar, auditoria interna e ações de segurança;

VII – manter documentação, registros e trilhas de auditoria de forma íntegra e segura;

VIII – garantir conformidade com esta Norma e com normativos superiores.

Seção II – Das Chefias

Art. 43. Compete às chefias imediatas:

I – autorizar formalmente solicitações de acesso, alteração de perfil ou uso excepcional;

II – comunicar à CGTI desligamentos, afastamentos ou mudanças funcionais de forma imediata;

III – revisar periodicamente os acessos concedidos aos membros de sua equipe;

IV – responder por solicitações indevidas ou excessivas de acesso.

Seção III – Dos Gestores de Sistemas

Art. 44. Compete aos gestores de sistemas:

I – definir e manter matriz de perfis e requisitos de acesso;

II – validar solicitações de permissões sensíveis ou privilegiadas;

III – assegurar que logs de ações administrativas ou críticas sejam registrados;

IV – revisar permissões e acessos relevantes de maneira periódica.

Seção IV – Dos Usuários

Art. 45. Compete aos usuários:

I – utilizar credenciais de forma pessoal e intrans

II – comunicar imediatamente qualquer indício de violação, acesso suspeito ou incidente;

III – encerrar sessões antes de se ausentar do posto de trabalho;

IV – utilizar sistemas, serviços e credenciais exclusivamente para fins institucionais;

V – cumprir integralmente esta Norma e demais normativos correlatos.

DAS SANÇÕES

Art. 46. O descumprimento das regras estabelecidas nesta Norma constitui incidente de segurança da informação e será tratado conforme a Política de Segurança da Informação, sem prejuízo das responsabilidades administrativas, civis e penais cabíveis.

Art. 47. Poderão ser aplicadas ao usuário infrator, conforme a gravidade da conduta:

I – advertência formal;

II – bloqueio temporário ou definitivo de credenciais;

III – revogação de privilégios e acessos;

IV – instauração de procedimento disciplinar;

V – demais medidas previstas em lei ou regulamentos.

DISPOSIÇÕES FINAIS

Art. 48. Os casos omissos serão analisados tecnicamente pela CGTI e submetidos ao Subcomitê de Segurança da Informação para deliberação.

Art. 49. A interpretação desta Norma deverá observar a Política de Segurança da Informação, a legislação aplicável e os demais normativos internos do MCOM.

Art. 50. Esta Norma poderá ser revista ou atualizada a qualquer tempo, por iniciativa da CGTI ou do Subcomitê de Segurança da Informação, sempre que houver evolução tecnológica, mudança regulatória ou necessidade operacional.

ANEXO I

TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE

Pelo presente instrumento, eu_____ , CPF nº _____, documento de identidade nº_____, expedida pelo_____

, em_____, e lotado no Ministério das

Comunicações - MCOM, DECLARO, sob pena das sanções cabíveis nos termos da Política de Segurança da Informação - POSIC do MCOM que assumo a responsabilidade por:

I- tratar o(s) ativo(s) de informação como patrimônio do Ministério das Comunicações;

II- utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do MCOM;

III- contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação na Administração Pública Federal, direta e indireta, e dá outras providências;

IV- utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do MCOM;

V- responder, perante o MCOM, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

Brasília, __ de_____ de 20__.

Nome e assinatura do usuário:

Unidade de Lotação:

Nome e assinatura da Autoridade Responsável pela Autorização do Acesso:

ANEXO II

TERMO DE RESPONSABILIDADE - VPN

Pelo presente instrumento, eu _____, CPF nº _____, documento de identidade nº _____, expedida pelo _____, em _____, e lotado no Ministério das Comunicações - MCom, DECLARO, sob pena das sanções cabíveis nos termos da Política de Segurança da Informação - POSIC do MCom que estou ciente das seguintes responsabilidades:

I - é minha responsabilidade garantir que o acesso remoto à rede do MCom não seja utilizado por pessoas não autorizadas. Os dados fornecidos para acesso são pessoais e intransferíveis;

II - o acesso à rede do MCom não será utilizado a partir de equipamentos de uso público (cybercafés, business centers etc.);

III – é obrigatória a utilização do software de acesso via VPN do MCom. O aplicativo de instalação, bem como os procedimentos de instalação e configuração, será fornecido pela Central de Atendimento quando da concessão de acesso;

IV – a instalação de solução de antimalware é de minha responsabilidade;

V - o uso dos recursos da rede permanecerá sujeito às diretrizes de segurança do MCom. A disponibilização desse acesso é condicionada ao atendimento, por parte de meus dispositivos, de critérios de segurança definidos pela CGTI;

VI - caso se confirme que a utilização do acesso remoto resultou em transtorno para a estrutura da rede do MCom, terei os direitos de acesso remoto suspensos. e

VII - serei responsabilizado por quaisquer incidentes de segurança gerados ativa ou passivamente pelo(s) equipamento(s) utilizado(s) para realizar a conexão remota à rede.

Unidade de lotação:

Justificativa para acesso:

Brasília,__de_____de 20__.

Nome do Servidor / Cargo

Nome Chefia Imediata /Cargo

Obs. O documento deve ser assinado pelo usuário e pela autoridade responsável (chefia imediata) pela autorização de acesso.

Documento assinado eletronicamente por **Gustavo Henrique de Souto Silva**, **Subsecretário de Tecnologia da Informação**, em 21/01/2026, às 11:06, 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 **13092299** e o código CRC **347DFF5A**.

Anexos

Não Possui.

Referência: Processo nº 53115.016204/2023-36 Documento nº 13092299