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

RESOLUÇÃO MCOM Nº 50, 28 DE OUTUBRO DE 2026

Aprova a Norma Complementar para o Uso Seguro do Correio Eletrônico Institucional.

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 art. 17 da Resolução nº 26/2024/MCOM, resolve:

Art. 1º Aprovar a Norma Complementar para o Uso Seguro do Correio Eletrônico Institucional, na forma do Anexo I desta Resolução.

Art. 2º Fica revogada a Portaria MCOM nº 3.858, de 14 de outubro de 2021.

Art. 3º 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 USO SEGURO DO CORREIO ELETRÔNICO INSTITUCIONAL

1. DO OBJETIVO

Art. 1º Esta Norma Complementar estabelece princípios, diretrizes, responsabilidades e requisitos de segurança para o uso, a administração, o monitoramento e a proteção do serviço de correio eletrônico institucional no âmbito do Ministério das Comunicações - MCOM.

Parágrafo único. O disposto nesta Norma tem por finalidade:

I - assegurar o uso adequado do correio eletrônico institucional;

II - proteger as informações produzidas, recebidas, armazenadas ou transmitidas por meio do serviço;

III - reduzir os riscos de acesso não autorizado, fraude, vazamento de informações, código malicioso, phishing, Business Email Compromise - BEC e demais ameaças cibernéticas;

IV - garantir a rastreabilidade e a adequada gestão do ciclo de vida das contas de correio eletrônico; e

V - promover a integração do serviço com os processos de segurança da informação, proteção de dados pessoais, gestão documental e tratamento de incidentes.

2. DA ABRANGÊNCIA

Art. 2º Esta Norma aplica-se:

I - às unidades organizacionais do Ministério das Comunicações;

II - aos agentes públicos, estagiários, colaboradores, consultores, prestadores de serviços, terceirizados e demais usuários autorizados a utilizar o serviço de correio eletrônico institucional;

III - aos fornecedores e prestadores de serviços que administrem, suportem ou utilizem o serviço de correio eletrônico institucional, quando cabível ao respectivo vínculo ou instrumento contratual; e

IV - às contas individuais, contas funcionais, caixas postais compartilhadas, listas de distribuição, grupos de comunicação e contas técnicas ou automatizadas mantidas ou autorizadas pelo Ministério.

3. DAS REFERÊNCIAS NORMATIVAS E TÉCNICAS

Art. 3º A aplicação desta Norma observará, especialmente:

I - Lei nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação;

II - Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais;

III - Decreto nº 11.856, de 26 de dezembro de 2023 - Política Nacional de Cibersegurança;

IV - Decreto nº 12.002, de 22 de abril de 2024;

V - Decreto nº 12.572, de 4 de agosto de 2025 - Política Nacional de Segurança da Informação;

VI - Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, e suas alterações;

VII - Portaria SGD/MGI nº 9.511, de 2025, e o Programa de Privacidade e Segurança da Informação - PPSI;

VIII - Política de Segurança da Informação do Ministério das Comunicações;

IX - Política de Governança do Ministério das Comunicações;

X - Norma Complementar para o Controle de Acesso Lógico;

XI - Norma Complementar para o Tratamento de Incidentes de Segurança da Informação;

XII - Norma Complementar para o Gerenciamento de Vulnerabilidades;

XIII - Norma Complementar para a Gestão de Riscos de Segurança da Informação;

XIV - normas institucionais de gestão documental, dispositivos móveis e proteção de dados pessoais; e

XV - demais normas legais, regulamentares e técnicas aplicáveis.

4. DOS CONCEITOS E DAS DEFINIÇÕES

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

I - conta individual: conta institucional vinculada a usuário determinado e de uso pessoal e intransferível;

II - conta funcional: conta vinculada a unidade, função, atividade ou serviço institucional, independentemente da pessoa que exerça determinada atribuição;

III - caixa postal compartilhada: recurso de correio eletrônico acessado por mais de um usuário autorizado, mediante credenciais individuais e rastreáveis;

IV - lista de distribuição: conjunto de endereços destinado ao envio de mensagens a grupo previamente definido;

V - conta técnica ou automatizada: conta destinada exclusivamente à execução de atividades sistêmicas, integrações ou envio automatizado de mensagens;

VI - correio eletrônico institucional: serviço disponibilizado ou autorizado pelo MCOM para envio, recebimento, armazenamento e gerenciamento de mensagens eletrônicas relacionadas às atividades institucionais;

VII - phishing: técnica de engenharia social utilizada para induzir o destinatário a fornecer informações, executar ações ou acessar conteúdos maliciosos;

VIII - Business Email Compromise - BEC: fraude que utiliza o comprometimento, a falsificação ou o uso indevido de identidade ou conta de correio eletrônico para induzir destinatários à realização de pagamentos, transferências, alteração de dados, compartilhamento de informações ou outras ações indevidas;

IX - comprometimento de conta: uso, controle ou acesso não autorizado a conta de correio eletrônico;

X - encaminhamento automático: regra destinada a redirecionar mensagens recebidas para outro endereço eletrônico;

XI - autenticação multifator - MFA: mecanismo que exige dois ou mais fatores independentes para validar a identidade do usuário;

XII - prevenção contra perda de dados - DLP: processos e ferramentas destinados a identificar, monitorar e impedir vazamento ou compartilhamento indevido de informações;

XIII - informação protegida: informação sujeita a restrição de acesso, sigilo, proteção de dados pessoais ou outro requisito específico de proteção previsto em legislação, regulamentação ou norma institucional; e

XIV - sistema IA-assistido: sistema que utiliza técnicas de Inteligência Artificial ou Aprendizado de Máquina para apoiar atividades de filtragem, detecção de ameaças, classificação, monitoramento ou proteção do correio eletrônico.

§ 1º Os demais conceitos observarão as definições constantes da Política de Segurança da Informação, da legislação e das normas institucionais aplicáveis.

§ 2º Em caso de divergência, prevalecerão as definições previstas em lei ou em regulamentação específica.

5. DAS DIRETRIZES GERAIS

Art. 5º O serviço de correio eletrônico institucional deverá observar, no mínimo, as seguintes diretrizes:

I - finalidade institucional;

II - proteção da confidencialidade, integridade, disponibilidade e autenticidade das informações;

III - autenticação individualizada e rastreável;

IV - privilégio mínimo e necessidade de conhecimento;

V - proteção de dados pessoais;

VI - registro e rastreabilidade das ações relevantes;

VII - segregação de responsabilidades;

VIII - prevenção e tratamento de incidentes;

IX - continuidade e disponibilidade do serviço;

X - proporcionalidade, transparência e finalidade no monitoramento;

XI - integração com a gestão de acessos, riscos, vulnerabilidades e ativos; e

XII - melhoria contínua dos controles de segurança.

Art. 6º O correio eletrônico institucional destina-se às atividades institucionais e administrativas do Ministério, devendo ser utilizado de forma compatível com a legislação, a segurança da informação, a proteção de dados pessoais e as normas institucionais aplicáveis.

Art. 7º As mensagens, os anexos, os documentos e os metadados produzidos ou recebidos no exercício das atribuições institucionais constituem informação institucional sob custódia do MCOM e submetem-se às regras de gestão documental, acesso à informação, proteção de dados pessoais e segurança da informação.

Parágrafo único. O disposto neste artigo não autoriza acesso indiscriminado ao conteúdo das comunicações nem afasta direitos de titulares de dados ou de terceiros protegidos pela legislação.

6. DAS CONTAS E DAS CAIXAS POSTAIS

Art. 8º A criação de contas de correio eletrônico dependerá de vínculo vigente, necessidade institucional e autorização conforme procedimento definido pela área responsável pela Tecnologia da Informação.

Art. 9º As contas deverão possuir:

I - finalidade definida;

II - responsável identificado;

III - acesso individualizado;

IV - permissões compatíveis com a necessidade funcional;

V - mecanismos de autenticação adequados ao risco; e

VI - registro de criação, alteração, delegação, bloqueio e encerramento.

Art. 10. As contas individuais são pessoais e intransferíveis, sendo vedados:

I - o compartilhamento de credenciais;

II - a utilização da conta por pessoa não autorizada; e

III - o uso de credenciais coletivas para acesso a caixas postais compartilhadas.

Art. 11. As contas funcionais, caixas postais compartilhadas, listas de distribuição e contas técnicas deverão possuir responsável formalmente designado.

§ 1º Compete ao responsável:

I - manter atualizada a relação de usuários autorizados;

II - solicitar a exclusão de acessos desnecessários;

III - assegurar que o recurso seja utilizado exclusivamente para sua finalidade; e

IV - comunicar alterações organizacionais que impactem a utilização da conta.

§ 2º O acesso a caixas postais compartilhadas deverá ocorrer por meio de credenciais individuais e rastreáveis.

Art. 12. As contas técnicas ou automatizadas:

I - deverão ser utilizadas exclusivamente para a finalidade autorizada;

II - não poderão ser utilizadas para comunicação pessoal;

III - deverão possuir credenciais protegidas e gerenciadas de forma segura;

IV - deverão ser periodicamente revisadas; e

V - não poderão possuir privilégios superiores aos necessários.

7. DO CICLO DE VIDA DAS CONTAS

Art. 13. O ciclo de vida das contas compreenderá, no mínimo:

I - solicitação;

II - autorização;

III - criação;

IV - concessão de acesso;

V - alteração;

VI - revisão periódica;

VII - suspensão ou bloqueio;

VIII - retenção, quando aplicável; e

IX - encerramento.

Art. 14. A unidade responsável pela gestão de pessoas e os gestores ou fiscais de contratos deverão comunicar tempestivamente à área de Tecnologia da Informação:

I - ingresso de usuário;

II - alteração de lotação, função ou atribuições;

III - afastamento que exija suspensão do acesso;

IV - encerramento de vínculo; e

V - qualquer evento que demande alteração ou revogação de acesso.

Art. 15. O acesso à conta deverá ser bloqueado tempestivamente após o encerramento do vínculo ou da necessidade institucional.

§ 1º O bloqueio da autenticação não implica eliminação imediata da caixa postal.

§ 2º A retenção, delegação, preservação, redirecionamento ou exclusão da caixa postal observará:

I - a necessidade administrativa;

II - a legislação aplicável;

III - as normas de gestão documental;

IV - a proteção de dados pessoais;

V - eventual determinação judicial ou administrativa; e

VI - procedimento operacional específico.

Art. 16. A delegação temporária de acesso deverá:

I - possuir justificativa formal;

II - ser limitada ao período necessário;

III - identificar os usuários autorizados;

IV - preservar a rastreabilidade; e

V - ser revogada ao término da necessidade.

8. DO USO ADEQUADO

Art. 17. O usuário deverá:

I - utilizar o serviço de forma ética, legal e compatível com as atividades institucionais;

II - proteger suas credenciais e mecanismos de autenticação;

III - conferir destinatários antes do envio;

IV - utilizar com cautela as funções "Responder a todos", cópia e cópia oculta;

V - observar a classificação e os requisitos de proteção da informação;

VI - limitar o conteúdo e os destinatários ao necessário para a finalidade da comunicação;

VII - utilizar assinatura institucional conforme padrão definido;

VIII - comunicar mensagens suspeitas, falhas ou comportamentos anômalos;

IX - não aprovar solicitações de autenticação multifator que não tenham sido iniciadas pelo próprio usuário;

X - seguir as orientações da área de Tecnologia da Informação e da ETIR; e

XI - registrar no SEI ou no repositório institucional correspondente as mensagens que constituam evidência de decisão, autorização, orientação ou ato administrativo relevante.

Art. 18. O correio eletrônico não substitui o Sistema Eletrônico de Informações - SEI nos atos, documentos, decisões e comunicações que devam integrar processo administrativo.

9. DAS VEDAÇÕES

Art. 19. É vedado utilizar o correio eletrônico institucional para:

I - prática de ato ilícito ou contrário às normas institucionais;

II - envio de conteúdo discriminatório, ofensivo, difamatório, ameaçador, pornográfico, fraudulento ou que configure assédio;

III - promoção político-partidária ou comercial estranha às atribuições institucionais, ressalvadas as comunicações autorizadas e os direitos assegurados em lei;

IV - disseminação de mensagens em cadeia, publicidade não autorizada ou conteúdo sem relação com as atividades institucionais;

V - envio intencional de código malicioso;

VI - tentativa de obter acesso não autorizado a sistemas ou informações;

VII - compartilhamento de senhas, códigos de autenticação, chaves, tokens ou outros segredos;

VIII - encaminhamento automático de mensagens para contas externas não autorizadas;

IX - envio de informação institucional para conta pessoal, salvo situação excepcional, formalmente justificada e autorizada, observados os controles de segurança aplicáveis;

X - cadastro da conta institucional em serviço externo sem necessidade funcional ou autorização;

XI - utilização de serviço externo de armazenamento, transferência ou compartilhamento não autorizado;

XII - envio de dados pessoais, informações sensíveis ou classificadas sem observância dos controles aplicáveis;

XIII - contorno, desativação ou alteração não autorizada de mecanismos de segurança, retenção, auditoria ou prevenção contra perda de dados;

XIV - falsificação ou ocultação indevida da identidade do remetente;

XV - acesso à caixa postal de outro usuário sem autorização; e

XVI - qualquer uso que comprometa a segurança, a disponibilidade ou a imagem institucional.

Art. 20. É vedada a cessão, disponibilização ou utilização da lista de endereços de correio eletrônico institucional por pessoa ou entidade externa ao MCOM, salvo quando necessária à finalidade institucional, amparada por competência legal ou formalmente autorizada.

10. DOS REQUISITOS E DOS CONTROLES DE SEGURANÇA

Art. 21. O serviço de correio eletrônico deverá implementar, conforme aplicável e de acordo com os riscos, os seguintes controles técnicos e administrativos:

I - autenticação multifator para acessos interativos;

II - bloqueio de mecanismos de autenticação considerados inseguros ou obsoletos;

III - controle de sessões;

IV - mecanismos de autenticação e proteção dos domínios de correio eletrônico;

V - criptografia em trânsito mediante protocolos seguros;

VI - filtragem antispam, antiphishing e antimalware;

VII - análise de links, anexos e conteúdos potencialmente maliciosos, inclusive por mecanismos de sandbox, quando tecnicamente aplicável;

VIII - mecanismos de prevenção contra perda e exfiltração de informações, de forma proporcional ao risco;

IX - proteção contra falsificação de identidade, comprometimento de conta e domínios semelhantes;

X - registro, monitoramento e correlação de eventos relevantes;

XI - detecção de comportamentos anômalos;

XII - proteção contra tentativas automatizadas de acesso;

XIII - revisão periódica de permissões, regras e encaminhamentos;

XIV - atualização e correção dos componentes do serviço; e

XV - mecanismos de continuidade, recuperação, retenção e preservação.

§ 1º A autenticação multifator será obrigatória para os acessos interativos, ressalvadas situações técnicas devidamente justificadas e submetidas a controle equivalente.

§ 2º As contas técnicas não interativas deverão adotar mecanismos de autenticação e proteção compatíveis com sua finalidade e risco.

§ 3º Os mecanismos de autenticação e proteção de domínio serão definidos em procedimento técnico e poderão incluir SPF, DKIM, DMARC ou tecnologias que venham a substituí-los ou complementá-los.

Art. 22. Os parâmetros técnicos, os limites de armazenamento, os tipos de arquivos permitidos, o tamanho de anexos, as regras de filtragem, os requisitos de retenção e demais configurações operacionais serão definidos e divulgados pela área responsável pela Tecnologia da Informação em procedimento próprio.

11. DA PROTEÇÃO CONTRA PHISHING, BEC E COMPROMETIMENTO DE CONTAS

Art. 23. Os usuários deverão adotar cautela especial quanto a mensagens que:

I - solicitem credenciais, códigos de autenticação ou informações sensíveis;

II - contenham links, QR Codes ou anexos inesperados;

III - apresentem urgência, ameaça ou oferta incompatível com a comunicação habitual;

IV - simulem páginas de autenticação;

V - solicitem alteração de dados bancários, pagamentos, transferências ou mudanças de beneficiário;

VI - utilizem domínio, endereço ou identidade semelhante à de remetente legítimo;

VII - provoquem solicitações inesperadas de autenticação multifator; ou

VIII - apresentem características compatíveis com phishing, spear-phishing, BEC ou outro tipo de engenharia social.

Art. 24. Na suspeita de phishing, BEC, comprometimento de conta ou envio indevido de informação, o usuário deverá:

I - interromper a interação com a mensagem;

II - comunicar imediatamente a ETIR pelos canais institucionais;

III - preservar a mensagem e demais evidências;

IV - alterar as credenciais, quando orientado;

V - encerrar sessões ativas, quando aplicável; e

VI - cumprir as medidas de contenção determinadas pela ETIR ou pela área responsável pela Tecnologia da Informação.

Art. 25. O acesso à conta poderá ser suspenso cautelarmente quando houver indício de comprometimento, risco à segurança ou necessidade de contenção.

§ 1º A medida poderá ser determinada, coordenada ou executada pela ETIR ou pela área responsável pela Tecnologia da Informação, conforme suas competências e os procedimentos institucionais.

§ 2º A suspensão deverá ser registrada e comunicada às unidades competentes.

§ 3º A suspensão cautelar constitui medida de segurança e não possui natureza sancionatória, devendo permanecer apenas pelo período necessário à contenção, à análise e à recuperação segura da conta.

Art. 26. A área responsável pela Tecnologia da Informação e a ETIR poderão, conforme suas competências, em situação de risco ou incidente:

I - bloquear mensagens, anexos, endereços, domínios ou links;

II - suspender temporariamente contas ou sessões;

III - revogar credenciais ou tokens;

IV - remover regras de encaminhamento maliciosas;

V - restringir o envio ou recebimento de mensagens; e

VI - adotar outras medidas técnicas necessárias à contenção.

Parágrafo único. As ações deverão ser registradas e comunicadas aos responsáveis, observadas a urgência, a proporcionalidade e a necessidade de preservação de evidências.

12. DA PROTEÇÃO DE DADOS E DAS INFORMAÇÕES

Art. 27. O envio de informações pelo correio eletrônico deverá observar:

I - a necessidade e a finalidade institucional;

II - a classificação e os requisitos de proteção da informação;

III - a minimização dos dados pessoais;

IV - a conferência dos destinatários;

V - o uso de canal ou mecanismo de proteção compatível com a sensibilidade do conteúdo;

VI - a restrição de acesso às pessoas que necessitem conhecer a informação; e

VII - os requisitos legais, regulamentares, contratuais e as orientações institucionais aplicáveis à proteção de dados pessoais.

Art. 28. Dados pessoais sensíveis, informações classificadas, sigilosas, estratégicas ou outros conteúdos de elevado impacto somente poderão ser transmitidos quando estritamente necessário e mediante controles compatíveis com o risco.

Parágrafo único. Os controles poderão incluir, conforme o caso:

I - criptografia;

II - controle de acesso baseado em identidade;

III - prevenção contra perda de dados;

IV - proteção do anexo por mecanismo aprovado;

V - restrição de encaminhamento, cópia, impressão ou download; e

VI - uso de repositório institucional seguro em substituição ao anexo.

Art. 29. O envio incorreto de mensagem, informação ou documento deverá ser comunicado imediatamente à ETIR, para avaliação e tratamento conforme a Norma Complementar para o Tratamento de Incidentes de Segurança da Informação.

Parágrafo único. Quando houver dados pessoais envolvidos, serão observados os procedimentos de comunicação e tratamento previstos na regulamentação de proteção de dados pessoais e na Norma Complementar para o Tratamento de Incidentes de Segurança da Informação.

13. DOS ANEXOS, DOS LINKS E DO COMPARTILHAMENTO DE ARQUIVOS

Art. 30. Os anexos, links e arquivos compartilhados poderão ser submetidos a inspeção, bloqueio, quarentena, análise adicional ou remoção pelos mecanismos de segurança do Ministério.

Art. 31. Arquivos que excedam os limites do serviço ou que exijam controles adicionais deverão ser disponibilizados por meio de repositório institucional autorizado ou outro mecanismo aprovado pela área responsável pela Tecnologia da Informação.

Art. 32. É vedado utilizar serviço externo não autorizado para transferência, armazenamento ou compartilhamento de informação institucional.

Parágrafo único. Exceções dependerão de justificativa, avaliação de risco e autorização conforme procedimento institucional.

14. DO ACESSO REMOTO E DOS DISPOSITIVOS MÓVEIS

Art. 33. O acesso remoto ao correio eletrônico deverá observar a Norma Complementar para o Controle de Acesso Lógico e os requisitos definidos pela área responsável pela Tecnologia da Informação.

Art. 34. O acesso ao correio eletrônico por dispositivos móveis, inclusive dispositivos pessoais autorizados, deverá observar a norma institucional específica de uso de dispositivos móveis, os controles de gerenciamento definidos pela área responsável pela Tecnologia da Informação e os requisitos de proteção aplicáveis às informações acessadas.

15. DO MONITORAMENTO E DA AUDITORIA

Art. 35. O serviço de correio eletrônico poderá ser monitorado para fins de:

I - segurança da informação;

II - disponibilidade e desempenho;

III - prevenção e tratamento de incidentes;

IV - investigação regularmente autorizada;

V - conformidade;

VI - atendimento de obrigações legais; e

VII - proteção do patrimônio e das informações do Ministério.

§ 1º O monitoramento e a auditoria deverão possuir finalidade definida, acesso restrito, necessidade, proporcionalidade, segregação de funções, rastreabilidade das consultas e prazo de retenção, observados os direitos fundamentais e a proteção de dados pessoais.

§ 2º Os registros técnicos e trilhas de auditoria deverão ser protegidos contra acesso, alteração ou eliminação não autorizados.

Art. 36. O acesso ao conteúdo das mensagens não constitui atividade ordinária e dependerá de:

I - motivação;

II - autorização da autoridade competente;

III - necessidade de conhecimento;

IV - registro da ação;

V - preservação da confidencialidade; e

VI - observância da legislação e dos procedimentos institucionais aplicáveis.

16. DOS SISTEMAS IA-ASSISTIDOS E DOS SERVIÇOS EXTERNOS

Art. 37. Poderão ser utilizados sistemas IA-assistidos para apoiar:

I - detecção de phishing, spam e código malicioso;

II - análise de links e anexos;

III - identificação de comportamento anômalo;

IV - classificação de mensagens;

V - prevenção de exfiltração; e

VI - priorização de alertas.

§ 1º A utilização de sistemas IA-assistidos deverá observar supervisão humana, segurança, rastreabilidade, proteção de dados pessoais e gestão de riscos.

§ 2º Os resultados, alertas ou recomendações produzidos por sistemas IA-assistidos que possam subsidiar bloqueio relevante, investigação ou responsabilização deverão ser submetidos à validação humana por agente autorizado antes de sua utilização, ressalvadas as medidas automatizadas de contenção previamente aprovadas.

Art. 38. É vedado encaminhar, inserir ou disponibilizar em serviços externos não autorizados, inclusive plataformas de Inteligência Artificial:

I - credenciais ou segredos de autenticação;

II - dados pessoais;

III - informações classificadas, sigilosas ou sensíveis;

IV - documentos internos não destinados à divulgação; e

V - conteúdo institucional cuja utilização externa não tenha sido autorizada.

17. DOS EVENTOS E DOS INCIDENTES

Art. 39. Os eventos e incidentes relacionados ao correio eletrônico deverão ser comunicados e tratados conforme a Norma Complementar para o Tratamento de Incidentes de Segurança da Informação.

Art. 40. A ETIR poderá emitir alertas, orientações, recomendações e determinações técnicas destinadas à prevenção ou à contenção de incidentes.

Art. 41. Incidentes envolvendo prestadores de serviços, infraestrutura contratada ou serviços em nuvem deverão observar, além desta Norma, as cláusulas contratuais e os requisitos de segurança definidos pelo Ministério.

18. DOS PAPÉIS E DAS RESPONSABILIDADES

Do Comitê de Governança Digital, Segurança da Informação e Proteção de Dados Pessoais - CGSP

Art. 42. Compete ao CGSP:

I - aprovar diretrizes institucionais relacionadas ao uso seguro do correio eletrônico;

II - acompanhar indicadores estratégicos e riscos relevantes;

III - deliberar sobre matérias estratégicas submetidas pelo Gestor de Segurança da Informação; e

IV - promover a integração desta Norma com a governança digital, a segurança da informação e a proteção de dados pessoais.

Do Subcomitê de Segurança da Informação - SINF

Art. 43. Compete ao SINF:

I - assessorar tecnicamente o CGSP;

II - analisar propostas de aperfeiçoamento;

III - acompanhar indicadores relacionados ao uso seguro do serviço; e

IV - propor ações de capacitação e fortalecimento dos controles.

Do Gestor de Segurança da Informação

Art. 44. Compete ao Gestor de Segurança da Informação:

I - coordenar institucionalmente a aplicação desta Norma;

II - aprovar procedimentos complementares de segurança;

III - acompanhar riscos e incidentes relevantes;

IV - promover a integração com os demais processos de Segurança da Informação; e

V - submeter ao CGSP matérias que demandem deliberação estratégica.

Da área responsável pela Tecnologia da Informação

Art. 45. Compete à área responsável pela Tecnologia da Informação:

I - administrar o serviço de correio eletrônico;

II - implementar e manter os controles técnicos;

III - gerenciar o ciclo de vida das contas;

IV - manter a disponibilidade e a continuidade do serviço;

V - definir e divulgar parâmetros operacionais;

VI - executar bloqueios, suspensões e revogações, observadas as competências institucionais;

VII - manter registros técnicos e trilhas de auditoria;

VIII - analisar a capacidade e o desempenho do serviço; e

IX - prestar suporte aos usuários.

Da Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR

Art. 46. Compete à ETIR:

I - receber e analisar comunicações de mensagens suspeitas;

II - tratar incidentes relacionados ao correio eletrônico;

III - determinar, coordenar ou recomendar medidas emergenciais de contenção, conforme suas competências;

IV - preservar evidências, quando aplicável;

V - emitir alertas e orientações;

VI - apoiar a recuperação de contas comprometidas; e

VII - propor melhorias nos controles de segurança.

Da unidade responsável pela Gestão de Pessoas

Art. 47. Compete à unidade responsável pela Gestão de Pessoas comunicar tempestivamente os eventos funcionais que impliquem criação, alteração, suspensão ou encerramento de contas.

Dos gestores e fiscais de contratos

Art. 48. Compete aos gestores e fiscais de contratos:

I - comunicar admissões, substituições, afastamentos e desligamentos de prestadores de serviços;

II - verificar se as contas e os acessos são compatíveis com a necessidade contratual; e

III - solicitar a revogação dos acessos ao término da necessidade.

Da unidade responsável pela Comunicação Social

Art. 49. Compete à unidade responsável pela Comunicação Social definir, quando aplicável, os padrões de identidade visual das assinaturas e das comunicações institucionais.

Parágrafo único. Os prestadores de serviços deverão utilizar assinatura compatível com seu vínculo contratual, de forma a não induzir o destinatário a erro quanto à sua condição funcional.

Das unidades organizacionais

Art. 50. Compete às unidades organizacionais:

I - solicitar e justificar contas funcionais, caixas compartilhadas e listas;

II - designar seus responsáveis;

III - manter atualizada a relação de usuários autorizados;

IV - comunicar alterações que impactem os acessos; e

V - orientar os usuários quanto à utilização adequada do serviço.

Dos usuários

Art. 51. Compete aos usuários:

I - cumprir esta Norma e os procedimentos aplicáveis;

II - proteger suas credenciais;

III - utilizar o serviço de forma adequada;

IV - conferir destinatários e conteúdos antes do envio;

V - comunicar mensagens suspeitas, eventos e incidentes;

VI - seguir as orientações da ETIR e da área de Tecnologia da Informação; e

VII - responder pelas ações executadas por meio de sua conta, ressalvados os casos comprovados de comprometimento não imputável ao usuário.

19. DA CAPACITAÇÃO E DA CONSCIENTIZAÇÃO

Art. 52. O Ministério promoverá ações periódicas de capacitação e conscientização sobre:

I - phishing, BEC e engenharia social;

II - proteção de credenciais e autenticação multifator;

III - envio seguro de informações;

IV - proteção de dados pessoais;

V - uso de anexos e links;

VI - comunicação de incidentes; e

VII - uso seguro de dispositivos móveis e serviços externos.

Parágrafo único. Os usuários deverão participar das ações obrigatórias de conscientização e das simulações institucionais de segurança quando formalmente convocados.

20. DA CONFORMIDADE E DA RESPONSABILIZAÇÃO

Art. 53. O descumprimento desta Norma deverá ser comunicado ao Gestor de Segurança da Informação para avaliação e encaminhamento às instâncias competentes, conforme a natureza da ocorrência.

Art. 54. O descumprimento desta Norma será apurado pelas instâncias competentes, observados o devido processo legal, o contraditório, a ampla defesa, a proporcionalidade, o nexo causal e a legislação aplicável.

Parágrafo único. A mera ocorrência de incidente, comprometimento de conta, envio indevido ou vazamento de informação não implica responsabilização automática do usuário, devendo ser consideradas a conduta, as circunstâncias do caso, os controles disponibilizados e a eventual existência de comprometimento não imputável ao usuário.

Art. 55. A responsabilização administrativa, civil ou penal, quando cabível, não afasta as medidas técnicas de contenção, preservação de evidências, recuperação do serviço e comunicação de incidentes.

21. DO MONITORAMENTO E DA MELHORIA CONTÍNUA

Art. 56. A área responsável pela Tecnologia da Informação deverá monitorar a efetividade dos controles do serviço, considerando, quando aplicável:

I - disponibilidade;

II - volume de mensagens bloqueadas;

III - ocorrências de phishing, BEC e código malicioso;

IV - contas comprometidas;

V - tentativas de acesso não autorizado;

VI - incidentes de envio indevido ou exfiltração;

VII - tempo de bloqueio ou recuperação de contas; e

VIII - ações de melhoria implementadas.

Art. 57. Os indicadores e riscos relevantes deverão subsidiar:

I - a revisão dos controles;

II - a gestão de riscos;

III - o tratamento de vulnerabilidades;

IV - as ações de capacitação; e

V - a melhoria contínua do serviço.

22. DAS DISPOSIÇÕES FINAIS

Art. 58. Os procedimentos necessários à execução desta Norma serão elaborados pelas unidades responsáveis, no âmbito de suas competências, e aprovados pelo Gestor de Segurança da Informação quando relacionados à segurança do serviço.

Art. 59. Os casos omissos serão resolvidos pelo Gestor de Segurança da Informação, podendo ser submetidos ao SINF ou ao CGSP, conforme a natureza e a relevância da matéria.

Art. 60. Esta Norma deverá ser revisada:

I - periodicamente, conforme o planejamento de revisão da Política de Segurança da Informação;

II - quando houver alteração relevante da legislação, da estrutura organizacional ou da tecnologia utilizada;

III - em decorrência de incidentes relevantes;

IV - quando identificada oportunidade de aperfeiçoamento dos controles; ou

V - quando houver alteração significativa dos riscos relacionados ao serviço.

Art. 61. Esta Norma entra em vigor na data definida no ato que a aprovar.

Documento assinado eletronicamente por **Gustavo Henrique de Souto Silva**, **Subsecretário de Tecnologia da Informação**, em 29/10/2026, às 17:21, 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 **13600320** e o código CRC **3F5B6A04**.

Anexos

Não Possui.