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

RESOLUÇÃO MCOM Nº 49, 28 DE OUTUBRO DE 2026

Aprova a Norma Complementar para o Tratamento de Incidentes 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 art. 17 da Resolução nº 26/2024/MCOM, resolve:

Art. 1º Aprovar a Norma Complementar para o Tratamento de Incidentes de Segurança da Informação, na forma do Anexo I desta Resolução.

Art. 2º Fica revogada a Resolução nº 32/2025/MCOM, de 6 de fevereiro de 2025.

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 TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1. DO OBJETIVO

Art. 1º Esta Norma Complementar estabelece princípios, diretrizes, responsabilidades e requisitos para o tratamento de incidentes de segurança da informação no âmbito do Ministério das Comunicações - MCOM, visando assegurar resposta coordenada, tempestiva e eficaz aos incidentes que possam comprometer a confidencialidade, integridade, disponibilidade ou autenticidade das informações e dos ativos de informação.

2. DA ABRANGÊNCIA

Art. 2º Esta Norma aplica-se:

I - aos órgãos e unidades do Ministério das Comunicações;

II - aos servidores públicos, militares, empregados públicos, estagiários, colaboradores, terceirizados, consultores e demais usuários que utilizem ativos de informação do Ministério; e

III - aos prestadores de serviços e fornecedores que tratem informações ou utilizem ativos de informação do Ministério, quando previsto contratualmente.

3. DAS REFERÊNCIAS NORMATIVAS E TÉCNICAS

Art. 3º Esta Norma observa, entre outros, os seguintes instrumentos normativos e referências técnicas:

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

II - Decreto nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos;

III - Portaria GSI/PR nº 120, de 21 de dezembro de 2022, que aprova o Plano de Gestão de Incidentes Cibernéticos para a Administração Pública Federal - Plangic;

IV - Resolução CD/ANPD nº 15, de 24 de abril de 2024, que aprova o Regulamento de Comunicação de Incidente de Segurança;

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

VI - Política de Governança do Ministério das Comunicações;

VII - ato de instituição da Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR do Ministério das Comunicações;

VIII - National Institute of Standards and Technology - NIST, Special Publication 800-61, Revision 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, de abril de 2025;

IX - National Institute of Standards and Technology - NIST, The NIST Cybersecurity Framework - CSF 2.0, de fevereiro de 2024;

X - National Institute of Standards and Technology - NIST, Artificial Intelligence Risk Management Framework - AI RMF 1.0;

XI - National Institute of Standards and Technology - NIST, Internal Report 8596, Cybersecurity Framework Profile for Artificial Intelligence - Cyber AI Profile, em sua versão preliminar vigente, como referência técnica orientativa, no que couber ao uso de sistemas IA-assistidos;

XII - ISO/IEC 27035-1:2023, Information Technology - Information Security Incident Management - Part 1: Principles and Process, e demais partes aplicáveis da série ISO/IEC 27035; e

XIII - demais normas legais, regulamentares, institucionais e referências técnicas correlatas à segurança da informação, à segurança cibernética e à proteção de dados pessoais aplicáveis.

4. DOS CONCEITOS E DEFINIÇÕES

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

I - Evento de Segurança da Informação: ocorrência identificada em sistema, serviço, rede, processo ou ativo de informação que possa indicar falha de controle, violação de política de segurança, situação anômala ou circunstância relevante para a segurança da informação, ainda que não caracterizada como incidente;

II - Incidente de Segurança da Informação: um ou mais eventos de segurança da informação que comprometam ou possam comprometer a confidencialidade, integridade, disponibilidade ou autenticidade das informações, dos serviços ou dos ativos de informação do Ministério;

III - Incidente Cibernético: incidente de segurança da informação ocorrido no ambiente cibernético que comprometa ou possa comprometer sistemas, redes, serviços, processos, dados ou infraestruturas tecnológicas;

IV - Incidente envolvendo Dados Pessoais: evento adverso confirmado relacionado à violação da confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais tratados pelo Ministério ou em seu nome;

V - Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR: equipe responsável por receber, registrar, analisar, classificar, tratar e responder às notificações e atividades relacionadas a

incidentes cibernéticos no âmbito do Ministério, bem como coordenar tecnicamente as ações de contenção, erradicação, recuperação e melhoria;

VI - Ativo de Informação: recurso, dado, informação, sistema, serviço, equipamento, infraestrutura, processo, pessoa ou ambiente que possua valor para o Ministério e que necessite de proteção;

VII - Ativo Crítico: ativo de informação cuja indisponibilidade, perda, destruição, alteração, divulgação ou acesso não autorizado possa causar impacto elevado ou crítico à missão institucional, à continuidade dos serviços, ao cumprimento de obrigações legais ou regulatórias ou à imagem do Ministério;

VIII - Evidência Digital: informação ou dado armazenado, processado ou transmitido em formato digital que possa contribuir para demonstrar a ocorrência, a origem, a extensão, o impacto ou outras circunstâncias relacionadas a um incidente de segurança da informação;

IX - Funções do NIST Cybersecurity Framework - CSF 2.0: as seis funções basilares da gestão de risco de segurança cibernética - Governar, Identificar, Proteger, Detectar, Responder e Recuperar;

X - Comprometimento: situação na qual a confidencialidade, integridade, disponibilidade ou autenticidade de informação, sistema, serviço, conta, credencial ou outro ativo tenha sido efetiva ou potencialmente violada;

XI - Vulnerabilidade: fragilidade, falha ou deficiência existente em ativo, sistema, processo, configuração, controle de segurança ou comportamento humano que possa ser explorada por uma ameaça e resultar em impacto adverso ao Ministério;

XII - Severidade do Incidente: grau atribuído ao incidente com base em critérios como impacto, abrangência, urgência, criticidade dos ativos afetados, possibilidade de propagação e repercussões operacionais, institucionais, legais, regulatórias, financeiras, reputacionais ou relacionadas à proteção de dados pessoais;

XIII - Crise Cibernética: situação decorrente de incidente cibernético de elevada severidade, abrangência ou complexidade, com potencial de comprometer significativamente a continuidade dos serviços, a missão institucional, ativos críticos ou a imagem do Ministério, demandando coordenação extraordinária e envolvimento da alta administração;

XIV - Contenção: conjunto de ações destinadas a limitar a propagação, reduzir o impacto e impedir o agravamento de um incidente, preservando, sempre que possível, as evidências necessárias à sua investigação;

XV - Erradicação: conjunto de ações destinadas a eliminar a causa, os mecanismos de persistência, os artefatos maliciosos, as vulnerabilidades exploradas e os demais elementos associados ao incidente;

XVI - Recuperação: conjunto de ações destinadas a restaurar, de forma segura e controlada, os sistemas, serviços, processos, dados e ativos afetados, incluindo a verificação de seu funcionamento e o monitoramento de eventual recorrência;

XVII - Comunicação Preliminar de Incidente: comunicação inicial realizada quando ainda não estiverem disponíveis todas as informações sobre o incidente, contendo os dados conhecidos no momento e sujeita a complementação posterior;

XVIII - Plano de Resposta a Incidentes: documento que estabelece a organização, os fluxos, as responsabilidades, os canais de comunicação, os critérios de escalonamento e as ações gerais necessárias à preparação, detecção, análise, contenção, erradicação, recuperação e avaliação de incidentes de segurança da informação;

XIX - Terceiro: pessoa física ou jurídica externa ao Ministério que, em razão de vínculo contratual, institucional ou de cooperação, trate informações, preste serviços ou tenha acesso a ativos de informação do Ministério;

XX - Fornecedor de Tecnologia ou de Segurança: terceiro responsável pelo fornecimento, operação, suporte, monitoramento, hospedagem, processamento ou proteção de sistemas, serviços,

infraestruturas ou informações do Ministério, incluindo prestadores de serviços gerenciados de segurança e provedores de computação em nuvem;

XXI - Prestador de Serviços Gerenciados de Segurança - MSSP: fornecedor especializado que executa, de forma continuada, atividades de monitoramento, detecção, análise, prevenção ou resposta a eventos e incidentes de segurança da informação;

XXII - Sistema IA-assistido: sistema que utiliza técnicas de Inteligência Artificial ou Aprendizado de Máquina para apoiar atividades de monitoramento, detecção, classificação, correlação de eventos, análise ou resposta a incidentes de segurança da informação, sem substituir a supervisão humana e a tomada de decisão pelos agentes públicos responsáveis;

XXIII - Responsabilidade Compartilhada: distribuição formal, contratual e operacional das atribuições relacionadas à prevenção, detecção, comunicação e resposta a incidentes entre o Ministério e terceiros, incluindo prestadores de serviços gerenciados de segurança, provedores de computação em nuvem e demais fornecedores;

XXIV - Lição Aprendida: conhecimento obtido a partir da análise de eventos, incidentes, exercícios ou simulações, destinado a identificar causas, falhas, oportunidades de melhoria e medidas corretivas ou preventivas;

XXV - Indicador de Comprometimento - IoC: dado, artefato ou padrão técnico que possa indicar a ocorrência ou tentativa de comprometimento de sistema, rede, conta, dispositivo ou outro ativo de informação;

XXVI - Procedimento Operacional de Resposta: documento que detalha atividades, responsabilidades, critérios, prazos, ferramentas, registros e fluxos específicos necessários ao tratamento de incidentes de segurança da informação;

XXVII - Parte Interessada: pessoa, unidade, órgão, entidade, autoridade ou organização que possa afetar, ser afetada ou possuir interesse no tratamento ou nos efeitos de um incidente de segurança da informação;

XXVIII - Gestor de Segurança da Informação: autoridade institucional responsável pela coordenação, supervisão e prestação de contas relativas ao processo de segurança da informação no Ministério, incluindo o tratamento de incidentes; e

XXIX - Controlador, Operador e Encarregado: figuras previstas no art. 5º, incisos VI, VII e VIII, da Lei nº 13.709, de 14 de agosto de 2018, aplicando-se, para os fins desta Norma, as definições e competências estabelecidas na referida Lei e na regulamentação da ANPD.

§ 1º Os conceitos previstos neste artigo deverão observar as definições constantes da Política de Segurança da Informação do Ministério, da legislação vigente, das normas institucionais e dos regulamentos específicos aplicáveis.

§ 2º Em caso de divergência entre as definições desta Norma e as estabelecidas em legislação ou regulamentação específica, prevalecerão as disposições legais ou regulamentares aplicáveis.

§ 3º Os procedimentos operacionais poderão estabelecer conceitos técnicos complementares, desde que não contrariem as definições e competências previstas nesta Norma.

5. DAS DIRETRIZES GERAIS

Art. 5º O tratamento de incidentes de segurança da informação deverá observar, no mínimo, as seguintes diretrizes:

I - atuação coordenada entre as unidades envolvidas;

II - resposta tempestiva aos incidentes identificados;

III - preservação da confidencialidade, integridade, disponibilidade e autenticidade das informações;

IV - preservação das evidências digitais, quando aplicável;

V - comunicação tempestiva às partes interessadas e às autoridades competentes, quando exigido por norma legal ou regulamentar;

VI - integração com os processos de gestão de riscos, gerenciamento de vulnerabilidades, continuidade de negócios, gestão de ativos e proteção de dados pessoais;

VII - registro, monitoramento e rastreabilidade das ações realizadas durante todo o ciclo de vida do incidente;

VIII - melhoria contínua dos processos de tratamento de incidentes; e

IX - observância dos princípios da proporcionalidade, rastreabilidade e responsabilização durante todo o tratamento do incidente.

Art. 6º O tratamento de incidentes deverá observar abordagem baseada em risco, considerando, entre outros aspectos:

I - criticidade do ativo afetado;

II - impacto institucional;

III - potencial comprometimento da missão institucional;

IV - possibilidade de propagação do incidente;

V - impactos à privacidade e à proteção de dados pessoais;

VI - impactos regulatórios, legais e reputacionais; e

VII - requisitos legais, regulatórios e contratuais aplicáveis.

6. DO PROCESSO DE TRATAMENTO DE INCIDENTES

Art. 7º O processo institucional de tratamento de incidentes adotará abordagem alinhada às Funções do NIST Cybersecurity Framework 2.0 - Governar, Identificar, Proteger, Detectar, Responder e Recuperar -, à NIST Special Publication 800-61, Revision 3, e à ISO/IEC 27035-1:2023, organizando-se operacionalmente em:

I - preparação;

II - detecção e registro;

III - análise e classificação;

IV - contenção;

V - erradicação;

VI - recuperação;

VII - lições aprendidas; e

VIII - melhoria contínua.

§ 1º Os procedimentos operacionais relativos a cada fase serão definidos pela ETIR e aprovados pelo Gestor de Segurança da Informação.

§ 2º Os procedimentos deverão observar as melhores práticas nacionais e internacionais aplicáveis ao tratamento de incidentes de segurança da informação.

§ 3º A comunicação e o registro constituem atividades transversais e permanentes, exercidas ao longo de todas as fases previstas nos incisos I a VIII, na forma dos arts. 8º, 12, 13 e 14.

§ 4º A melhoria contínua prevista no inciso VIII do caput também constitui atividade transversal e permanente, exercida durante e após cada incidente, na forma do art. 24.

7. DA CLASSIFICAÇÃO, DA COMUNICAÇÃO E DA NOTIFICAÇÃO DE INCIDENTES

Art. 8º Todo incidente de segurança da informação deverá ser registrado e comunicado à Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR, por meio dos canais institucionais estabelecidos.

§ 1º A comunicação deverá ocorrer tão logo o incidente seja identificado ou haja indícios suficientes de sua ocorrência.

§ 2º A omissão injustificada na comunicação de incidentes poderá sujeitar o responsável às medidas administrativas cabíveis.

§ 3º Conforme a severidade e a natureza do incidente, a comunicação e o tratamento envolverão, de forma coordenada, as áreas jurídica, de comunicação social, de gestão de pessoas e a alta administração, segundo os gatilhos de escalonamento definidos em procedimento operacional aprovado pelo Gestor de Segurança da Informação.

Art. 9º A ETIR poderá determinar, coordenar ou adotar, conforme as competências institucionais e nos limites estabelecidos em procedimento operacional previamente aprovado pelo Gestor de Segurança da Informação, medidas emergenciais de contenção destinadas a reduzir a propagação ou o impacto de incidente, incluindo isolamento de ativos, bloqueio de contas, revogação de credenciais, desconexão de rede e suspensão temporária de serviços.

Parágrafo único. As medidas adotadas deverão ser comunicadas imediatamente ao Gestor de Segurança da Informação e às unidades responsáveis pelos ativos ou serviços afetados, sem prejuízo da comunicação posterior às demais partes interessadas.

Art. 10. Os incidentes serão classificados de acordo com critérios estabelecidos em procedimento operacional aprovado pelo Gestor de Segurança da Informação, considerando, no mínimo:

I - criticidade do ativo afetado;

II - impacto operacional;

III - impacto institucional;

IV - impacto à confidencialidade, integridade, disponibilidade ou autenticidade da informação;

V - existência de dados pessoais envolvidos;

VI - possibilidade de propagação; e

VII - repercussão legal, regulatória ou reputacional.

Art. 11. A partir dos critérios previstos no art. 10, os incidentes serão classificados em quatro níveis de severidade - baixo, moderado, alto e crítico -, de acordo com metodologia institucional de priorização baseada em risco, observadas, como referência técnica, as recomendações da NIST Special Publication 800-61, Revision 3.

§ 1º Os parâmetros objetivos de enquadramento em cada nível, os prazos correspondentes, os gatilhos de escalonamento e as autoridades responsáveis serão definidos no mesmo procedimento operacional.

§ 2º A classificação inicial poderá ser reavaliada durante o ciclo de vida do incidente sempre que novas informações justificarem alteração de severidade, com registro fundamentado da mudança.

Art. 12. Os incidentes que envolvam dados pessoais, nos termos do inciso IV do art. 4º, deverão observar, além desta Norma e da classificação prevista nos arts. 10 e 11, a Lei nº 13.709, de 14 de agosto de 2018, e a regulamentação expedida pela Autoridade Nacional de Proteção de Dados - ANPD.

§ 1º Sempre que houver indícios de comprometimento de dados pessoais, a ETIR deverá comunicar imediatamente o Encarregado pelo Tratamento de Dados Pessoais.

§ 2º Compete ao Controlador avaliar a ocorrência de risco ou dano relevante aos titulares e deliberar quanto à necessidade de comunicação à ANPD e aos titulares, observado o disposto na legislação vigente.

§ 3º A ETIR prestará apoio técnico ao Controlador e ao Encarregado durante todo o processo de avaliação e tratamento do incidente.

§ 4º A avaliação da existência de risco ou dano relevante, a comunicação à ANPD e aos titulares, a complementação das informações e a manutenção dos registros observarão os critérios, prazos e requisitos estabelecidos na Resolução CD/ANPD nº 15, de 24 de abril de 2024, ou em norma que venha a substituí-la.

§ 5º A decisão quanto à comunicação ou à não comunicação do incidente deverá ser formalmente fundamentada e registrada pelo Controlador, com apoio técnico da ETIR e participação do Encarregado pelo Tratamento de Dados Pessoais.

§ 6º Os operadores deverão comunicar ao Ministério, sem demora injustificada e no prazo contratualmente estabelecido, os incidentes que envolvam dados pessoais tratados em nome do Ministério, fornecendo as informações necessárias ao cumprimento das obrigações do Controlador.

§ 7º A comunicação à ANPD e aos titulares poderá ser operacionalizada pelo Encarregado, quando formalmente definida pelo Controlador, sem transferência da responsabilidade legal atribuída ao Controlador.

Art. 13. Os procedimentos relativos à comunicação de incidentes aos órgãos competentes, parceiros institucionais, fornecedores, usuários e demais partes interessadas serão disciplinados em procedimento operacional aprovado pelo Gestor de Segurança da Informação, observada a classificação de severidade prevista no art. 11.

Art. 14. A ETIR deverá avaliar e realizar, quando aplicável, a notificação de incidentes cibernéticos ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov e aos demais órgãos competentes, conforme a natureza, a severidade, nos termos do art. 11, e o impacto do incidente, observados os normativos da Rede Federal de Gestão de Incidentes Cibernéticos, o Plano de Gestão de Incidentes Cibernéticos para a Administração Pública Federal - Plangic e os procedimentos institucionais.

Parágrafo único. A ETIR manterá canal institucional próprio para comunicação com o CTIR Gov, preferencialmente por meio de endereço eletrônico dedicado a incidentes de segurança.

8. DOS PAPÉIS E RESPONSABILIDADES

Art. 15. A governança do processo de tratamento de incidentes, em alinhamento à Função Governar do NIST CSF 2.0, compreende a definição de papéis e responsabilidades, a supervisão institucional, a observância do apetite e da tolerância a risco institucionalmente definidos, a adequada alocação de recursos e a prestação de contas, observadas as competências do CGSP e do Gestor de Segurança da Informação.

Parágrafo único. O Ministério assegurará, observadas as disponibilidades administrativas e orçamentárias, os recursos humanos, tecnológicos e materiais necessários ao funcionamento da ETIR e ao desempenho de suas atribuições.

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

Art. 16. Compete ao CGSP:

I - aprovar diretrizes institucionais para o tratamento de incidentes de segurança da informação;

II - acompanhar indicadores estratégicos relacionados aos incidentes de segurança da informação;

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

IV - promover a integração do tratamento de incidentes com os processos de governança digital, segurança da informação e proteção de dados pessoais.

Do Subcomitê de Segurança da Informação - SINF

Art. 17. Compete ao SINF:

I - assessorar tecnicamente o CGSP nas matérias relativas ao tratamento de incidentes;

II - analisar propostas de aperfeiçoamento dos processos de tratamento de incidentes;

III - acompanhar os resultados dos indicadores institucionais relacionados ao tratamento de incidentes;

IV - propor ações destinadas ao fortalecimento da capacidade institucional de resposta a incidentes; e

V - acompanhar a implementação das deliberações do CGSP relacionadas ao tratamento de incidentes.

Do Gestor de Segurança da Informação

Art. 18. Compete ao Gestor de Segurança da Informação:

I - coordenar institucionalmente o processo de tratamento de incidentes de segurança da informação;

II - supervisionar as atividades desempenhadas pela ETIR;

III - aprovar os procedimentos operacionais relativos ao tratamento de incidentes;

IV - acompanhar incidentes classificados como críticos ou de elevado impacto;

V - promover a integração entre a gestão de incidentes, a gestão de riscos, o gerenciamento de vulnerabilidades, a continuidade de negócios e a proteção de dados pessoais; e

VI - submeter ao CGSP matérias que demandem deliberação estratégica.

Da Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR

Art. 19. Compete à ETIR:

I - executar as atividades de tratamento de incidentes de segurança da informação;

II - monitorar, analisar, conter, erradicar e apoiar a recuperação dos incidentes, diretamente ou em coordenação com as unidades técnicas competentes;

III - registrar todas as atividades relacionadas ao tratamento dos incidentes;

IV - preservar evidências digitais, quando aplicável;

V - elaborar relatórios técnicos dos incidentes tratados;

VI - propor melhorias nos controles de segurança da informação;

VII - elaborar, manter e revisar os procedimentos operacionais relativos ao tratamento de incidentes; e

VIII - apoiar tecnicamente o Gestor de Segurança da Informação, o Controlador, o Encarregado pelo Tratamento de Dados Pessoais e as unidades envolvidas.

Da unidade responsável pela Tecnologia da Informação

Art. 20. Compete à unidade responsável pela Tecnologia da Informação:

I - apoiar tecnicamente a ETIR na detecção, análise e resposta a incidentes que envolvam ativos, sistemas, serviços ou infraestruturas sob sua administração;

II - executar, nos ativos e serviços sob sua administração, as medidas técnicas de contenção, erradicação e recuperação determinadas ou coordenadas pela ETIR, observadas as competências institucionais;

III - disponibilizar à ETIR, quando necessário ao tratamento do incidente, logs, registros, evidências e demais informações técnicas sob sua custódia;

IV - implementar e manter os controles técnicos necessários à prevenção, detecção e resposta a incidentes, de acordo com as normas institucionais e os procedimentos operacionais aplicáveis; e

V - apoiar a restauração segura dos serviços e ativos afetados, inclusive quanto às ações de continuidade e recuperação sob sua responsabilidade.

Das Unidades Organizacionais

Art. 21. Compete às unidades organizacionais do Ministério:

I - comunicar tempestivamente incidentes de segurança da informação;

II - apoiar a ETIR durante as atividades de investigação e tratamento;

III - implementar as medidas corretivas, preventivas e operacionais sob sua responsabilidade;

IV - preservar evidências e informações relacionadas ao incidente sempre que solicitado pela ETIR; e

V - colaborar na implementação das ações de melhoria decorrentes das lições aprendidas.

Dos Usuários

Art. 22. Compete aos usuários:

I - comunicar imediatamente qualquer evento ou incidente de segurança da informação de que tenham conhecimento;

II - observar as orientações emitidas pela ETIR durante o tratamento de incidentes;

III - preservar, sempre que possível, evidências relacionadas ao incidente; e

IV - utilizar adequadamente os ativos de informação do Ministério, observando a Política de Segurança da Informação e demais normas institucionais.

9. DO USO DE SISTEMAS IA-ASSISTIDOS

Art. 23. Poderão ser utilizados sistemas IA-assistidos para apoiar atividades relacionadas ao tratamento de incidentes de segurança da informação, incluindo:

I - detecção de eventos anômalos;

II - correlação de eventos de segurança;

III - apoio à classificação e à priorização de incidentes;

IV - apoio à análise técnica;

V - geração de recomendações para contenção, erradicação e recuperação; e

VI - apoio à elaboração de relatórios técnicos.

§ 1º A utilização de sistemas IA-assistidos não substitui a análise técnica nem a tomada de decisão pelos agentes públicos responsáveis.

§ 2º As recomendações produzidas por sistemas IA-assistidos deverão ser validadas por integrante da ETIR antes de sua adoção.

§ 3º A utilização de Inteligência Artificial deverá observar os princípios de transparência, supervisão humana, segurança, rastreabilidade, proteção de dados pessoais e gestão de riscos previstos na Política de Segurança da Informação e na regulamentação institucional aplicável.

§ 4º O uso de sistemas IA-assistidos considerará, no que couber, as diretrizes do NIST Artificial Intelligence Risk Management Framework - AI RMF e, como referência técnica orientativa enquanto permanecer em versão preliminar, o NIST IR 8596 - Cyber AI Profile.

§ 5º É vedada a inserção, em sistemas IA-assistidos não homologados pelo Ministério, de credenciais, evidências digitais, informações classificadas, dados protegidos por sigilo ou informações cujo tratamento possa comprometer a segurança institucional ou a proteção de dados pessoais.

§ 6º A contratação ou utilização de sistemas IA-assistidos deverá ser precedida de avaliação de riscos de segurança, privacidade, retenção, transferência, compartilhamento e reutilização dos dados pelo fornecedor.

§ 7º As recomendações produzidas por sistemas IA-assistidos, as decisões humanas de validação e as intervenções relevantes deverão ser registradas de forma rastreável, observado o princípio da necessidade e os requisitos de segurança aplicáveis.

10. DO MONITORAMENTO, DOS INDICADORES E DA MELHORIA CONTÍNUA

Art. 24. O processo de tratamento de incidentes será continuamente monitorado, avaliado e aperfeiçoado, sendo a melhoria contínua atividade transversal e permanente, exercida durante e após cada

incidente, com base em indicadores de desempenho, lições aprendidas e análise crítica dos incidentes ocorridos, dos exercícios realizados e das avaliações de maturidade.

Art. 25. O Gestor de Segurança da Informação deverá promover, periodicamente, a avaliação da efetividade do processo de tratamento de incidentes, considerando, no mínimo:

I - quantidade de incidentes registrados;

II - classificação e severidade dos incidentes;

III - tempo médio de detecção;

IV - tempo médio de resposta;

V - tempo médio de recuperação;

VI - percentual de incidentes resolvidos dentro do prazo estabelecido;

VII - reincidência de incidentes; e

VIII - percentual das ações corretivas implementadas.

Art. 26. Os incidentes tratados deverão subsidiar, sempre que aplicável:

I - a revisão da gestão de riscos de segurança da informação;

II - a atualização do processo de gerenciamento de vulnerabilidades;

III - a revisão do inventário e da classificação dos ativos de informação;

IV - a atualização dos planos de continuidade de negócios e de recuperação de desastres;

V - a revisão das medidas de proteção de dados pessoais; e

VI - o aprimoramento dos controles de segurança da informação.

Art. 27. A ETIR deverá elaborar relatórios gerenciais consolidados sobre os incidentes tratados, indicadores de desempenho, tendências observadas e oportunidades de melhoria.

§ 1º Os relatórios deverão subsidiar a tomada de decisão pelo Gestor de Segurança da Informação e pelo CGSP.

§ 2º Sempre que identificado incidente crítico ou com potencial impacto institucional relevante, deverá ser elaborado relatório específico contendo análise do incidente, impactos, medidas adotadas e recomendações.

Art. 28. Os registros dos incidentes, das evidências e dos relatórios técnicos e gerenciais serão retidos pelo prazo definido em procedimento operacional aprovado pelo Gestor de Segurança da Informação, observadas a legislação de proteção de dados pessoais, a legislação de acesso à informação, as normas de gestão documental do Ministério e as obrigações regulatórias aplicáveis.

11. DA CAPACITAÇÃO E DA CONSCIENTIZAÇÃO

Art. 29. O Ministério promoverá ações periódicas de capacitação e conscientização destinadas ao fortalecimento da cultura de tratamento de incidentes de segurança da informação.

Art. 30. O Ministério promoverá, com periodicidade mínima anual, exercícios de mesa e simulações técnicas de resposta a incidentes, contemplando, de forma alternada ou combinada e conforme avaliação de riscos, cenários como ransomware, indisponibilidade de serviços críticos, comprometimento de credenciais, incidentes envolvendo dados pessoais e incidentes envolvendo fornecedores e provedores de nuvem, com registro de resultados e planos de melhoria.

Art. 31. As ações de capacitação deverão contemplar, sempre que possível:

I - identificação e comunicação de incidentes;

II - preservação de evidências digitais;

III - resposta inicial a incidentes;

IV - proteção de dados pessoais durante o tratamento de incidentes;

V - boas práticas de segurança cibernética; e

VI - utilização dos canais institucionais de comunicação de incidentes.

12. DA CONFORMIDADE E DA RESPONSABILIZAÇÃO

Art. 32. O descumprimento das disposições desta Norma deverá ser comunicado ao Gestor de Segurança da Informação para avaliação das providências cabíveis.

Art. 33. A inobservância desta Norma poderá sujeitar os responsáveis às medidas administrativas, civis e penais previstas na legislação vigente, observado o devido processo legal.

Art. 34. A ocorrência de incidentes de segurança da informação decorrentes do descumprimento desta Norma deverá ser considerada nos processos de gestão de riscos, auditoria, controles internos e apuração de responsabilidade, quando aplicável.

13. DA GESTÃO DE EVIDÊNCIAS, DE TERCEIROS E DE VULNERABILIDADES REPORTADAS

Art. 35. As evidências relacionadas aos incidentes deverão ser preservadas quanto à confidencialidade, integridade, disponibilidade, autenticidade e cadeia de custódia, sempre que aplicável.

§ 1º A coleta e a preservação das evidências deverão assegurar, quando aplicável, o registro de sua origem, data e hora, responsável pela coleta, método de aquisição, verificação de integridade por mecanismo criptográfico, transferências de custódia, controles de acesso e condições de armazenamento.

§ 2º Os procedimentos deverão priorizar a preservação da evidência original e a realização das análises em cópias de trabalho ou imagens forenses, quando tecnicamente aplicável.

§ 3º Os procedimentos relativos à coleta, ao armazenamento, à preservação, ao acesso e ao descarte das evidências serão disciplinados em procedimento operacional aprovado pelo Gestor de Segurança da Informação, observadas as normas de proteção de dados pessoais e de acesso à informação.

§ 4º Havendo indícios de prática de ilícito penal relacionados ao incidente, a ETIR deverá comunicar imediatamente o Gestor de Segurança da Informação e a unidade institucional responsável para avaliação e adoção das providências cabíveis, assegurada a preservação das evidências.

Art. 36. Os contratos com prestadores de serviços, MSSP e provedores de nuvem que tratem informações ou administrem ativos do Ministério deverão prever, no que couber:

I - definição formal das responsabilidades compartilhadas para o tratamento de incidentes;

II - prazos e níveis de serviço para notificação de incidentes ao Ministério, sem demora injustificada;

III - obrigação de disponibilização ao Ministério de logs, registros e evidências necessários ao tratamento do incidente e, quando legalmente exigível, às autoridades competentes;

IV - obrigações de cooperação em atividades forenses, de contenção, de erradicação e de recuperação;

V - requisitos de segurança e de comunicação de incidentes na cadeia de suprimentos, inclusive quanto a subcontratados;

VI - vedação de descarte de logs e evidências após ciência de incidente potencial ou confirmado;

VII - regras de localização, retenção e devolução dos dados; e

VIII - obrigação de fornecer relatório de causa raiz e plano de ação corretiva.

Parágrafo único. Os requisitos previstos neste artigo deverão ser observados nas novas contratações e, quando juridicamente aplicável, nas prorrogações, renovações, alterações ou ajustes dos contratos vigentes.

Art. 37. O Ministério manterá canal formal para o recebimento de vulnerabilidades reportadas por terceiros, inclusive pesquisadores externos, cujo tratamento observará a Norma Complementar para o Gerenciamento de Vulnerabilidades.

§ 1º Quando a vulnerabilidade reportada caracterizar ou indicar possível incidente de segurança da informação, a ETIR deverá ser acionada conforme esta Norma.

§ 2º O procedimento institucional de recebimento de vulnerabilidades deverá observar os princípios de boa-fé, confidencialidade, resposta tempestiva e não retaliação aos pesquisadores que atuem de boa-fé e em conformidade com as regras nele estabelecidas.

14. DAS DISPOSIÇÕES FINAIS

Art. 38. Os procedimentos operacionais necessários à execução desta Norma serão elaborados pela ETIR, com a participação das unidades competentes, quando aplicável, e aprovados pelo Gestor de Segurança da Informação.

Art. 39. Incidentes que envolvam serviços contratados ou ativos administrados por terceiros deverão observar, além desta Norma, as cláusulas contratuais e os requisitos de segurança estabelecidos pelo Ministério.

Art. 40. Os casos omissos serão resolvidos pelo Gestor de Segurança da Informação, podendo ser submetidos ao Subcomitê de Segurança da Informação ou ao Comitê de Governança Digital, Segurança da Informação e Proteção de Dados Pessoais - CGSP, conforme a natureza e relevância da matéria.

Art. 41. Esta Norma deverá ser revisada:

I - sempre que houver alteração relevante da legislação ou dos normativos institucionais relacionados à segurança da informação;

II - em decorrência de incidentes de grande impacto que indiquem necessidade de aperfeiçoamento dos controles;

III - periodicamente, conforme planejamento institucional de revisão da Política de Segurança da Informação; ou

IV - quando identificado, em processo de melhoria contínua, oportunidade relevante de aperfeiçoamento do tratamento de incidentes.

Art. 42. 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 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 **13600273** e o código CRC **3FD91456**.

Anexos

Não Possui.