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

RESOLUÇÃO MCOM Nº 34, DE 29 DE MAIO DE 2025.

Aprova a Norma Complementar para Gestão e Auditoria de Conformidade em Segurança da Informação.

O SUBCOMITÊ DE SEGURANÇA DA INFORMAÇÃO instituído pela Portaria nº 8.490, de 24 de fevereiro de 2023, 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 Gestão e Auditoria de Conformidade em Segurança da Informação.

Art. 2º Esta Resolução entra em vigor no primeiro dia útil subsequente à data de sua publicação.

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

ANEXO I

NORMA COMPLEMENTAR PARA GESTÃO E AUDITORIA DE CONFORMIDADE EM SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO

Art. 1º Esta norma estabelece diretrizes e procedimentos para assegurar a gestão e auditoria eficaz da conformidade em segurança da informação, alinhada com as estratégias organizacionais e a gestão de riscos, assegurando o cumprimento das normas, regulamentos e melhores práticas aplicáveis. Seu foco está na proteção dos ativos de informação, prevenção de riscos e manutenção da integridade, confidencialidade e disponibilidade das informações, integrando-se com os objetivos estratégicos e operacionais do Ministério das Comunicações – MCOM.

2. ABRANGÊNCIA

Art. 2º Esta norma aplica-se a todos os servidores, prestadores de serviços, fornecedores e terceiros que possuam acesso ou utilizem sistemas, dados ou infraestrutura tecnológica do MCOM, abrangendo todos os processos internos e práticas externas relacionadas à segurança da informação.

Parágrafo único A norma se aplica a todas as ações, controles, sistemas e processos relacionados à segurança da informação, incluindo estratégias organizacionais e governança de riscos.

3. REFERÊNCIA LEGAL E NORMATIVA

Art. 3º As referências legais e normativas aplicáveis a esta norma são:

I - Instrução Normativa GSI/PR Nº 1, de 27 de maio de 2020 - Dispõe sobre a

Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

II - Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021 - Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

III - ABNT NBR ISO/IEC 27002:2022 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação;

IV - ABNT NBR ISO/IEC 27001:2022 - Sistema de Gestão da Segurança da Informação;

V - Norma Complementar nº 11/IN01/DSIC/GSIPR - Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF;

VI - Lei Geral de Proteção de Dados (LGPD), assegurando a conformidade com seus princípios, direitos dos titulares e requisitos para tratamento de dados pessoais quando aplicáveis.

4. PRINCÍPIOS

Art. 4º A gestão e auditoria de conformidade em segurança da informação será orientada pelos seguintes princípios:

I - Confidencialidade: Garantir que a informação esteja acessível apenas a indivíduos autorizados;

II - Integridade: Assegurar a precisão e confiabilidade das informações;

III - Disponibilidade: Garantir acesso às informações e serviços de TI sempre que necessário;

IV - Transparência: Assegurar a clareza e acessibilidade das normas e processos;

V - Melhoria Contínua: Evoluir constantemente os processos de segurança;

VI - Legalidade e Regulamentação: Garantir que todas as ações e políticas estejam alinhadas com leis, regulamentações e normas aplicáveis;

VII - Responsabilidade e Prestação de Contas: Definir claramente papéis e responsabilidades, garantindo que todas as partes cumpram suas obrigações;

VIII - Proporcionalidade: Assegurar que os controles sejam proporcionais ao risco envolvido, garantindo um equilíbrio entre segurança e operacionalidade;

IX - Resiliência: Promover a capacidade de adaptação e recuperação rápida diante de incidentes de segurança, incluindo a continuidade de negócios e recuperação de desastres;

X - Consistência e Padronização: Garantir que processos e controles sejam aplicados de maneira uniforme e coerente em toda a organização; e

XI - Cultura de Segurança: Estimular a conscientização e o comprometimento de todos os envolvidos com a segurança da informação, além de incluir a alta administração na formação de uma cultura de segurança.

5. DIRETRIZES GERAIS

Art. 5º A gestão e auditoria de conformidade em segurança da informação deverá ser orientada pelas seguintes diretrizes:

I - Implementação de controles de segurança apropriados para cada tipo de informação;

II - Definição de papéis e responsabilidades claros no processo de gestão e auditoria da conformidade;

III - Monitoramento e auditoria contínuos para assegurar a eficácia das medidas de segurança; e

IV - Aplicação de sanções em caso de descumprimento das diretrizes de segurança.

6. GESTÃO DE CONFORMIDADE E AUDITORIA DE CONFORMIDADE EM SEGURANÇA DA INFORMAÇÃO

Art. 6º A gestão de conformidade e a auditoria de conformidade em segurança da informação são dois processos distintos, mas complementares, fundamentais para a efetividade do sistema de segurança da informação.

§ 1 º Gestão de Conformidade em segurança da informação refere-se ao processo contínuo de implementação, monitoramento e aprimoramento das políticas, controles e práticas de segurança da informação, com foco na execução proativa e adaptação às mudanças no cenário organizacional.

§2º Auditoria de Conformidade em segurança da informação é a atividade independente com o objetivo de avaliar, verificar e assegurar que a gestão de conformidade em segurança da informação está sendo realizada de acordo com os parâmetros previstos, identificando lacunas e não conformidades.

7. PROCESSO DE GESTÃO DE CONFORMIDADE EM SEGURANÇA DA INFORMAÇÃO

Art. 7º O processo de gestão de conformidade em segurança da informação seguirá os seguintes passos:

I - Identificação e Classificação de Ativos: Avaliação e categorização conforme criticidade e riscos associados;

II - Avaliação de Riscos: Identificação e revisão periódica de riscos, considerando a evolução do ambiente tecnológico e regulamentar;

III - Implementação de Controles: Adoção de medidas administrativas, técnicas e físicas para mitigar os riscos;

IV - Monitoramento Contínuo: Utilização de sistemas de detecção e prevenção de intrusões, incluindo ferramentas automatizadas de segurança;

V - Auditoria de Conformidade em Segurança da Informação: Execução conforme procedimentos estabelecidos para assegurar a conformidade com as políticas e práticas de segurança.

8. AUDITORIA DE CONFORMIDADE EM SEGURANÇA DA INFORMAÇÃO

Art. 8º A auditoria de conformidade em segurança da informação será conduzida conforme os seguintes procedimentos:

I - Planejamento: Definição de escopo, metodologia e equipe responsável;

II - Execução: Revisão documental, entrevistas e testes para verificar a conformidade com as normas e controles;

III - Relatório de Auditoria: Registro de achados, riscos e recomendações para correção de não conformidades;

IV - Acompanhamento: Monitoramento das ações corretivas, com a apresentação de relatórios periódicos.

Art. 9º O tratamento de não conformidades será baseado nos seguintes critérios:

I - Critérios de Classificação: Estabelecimento de níveis de severidade (baixa, média, alta);

II - Prazos e Responsabilidades: Definição de responsáveis e prazos para cada etapa;

III - Registro de Ações e Lições Aprendidas: Criação de um histórico para melhoria contínua.

9. MATRIZ DOS PROCESSOS DE GESTÃO DE CONFORMIDADE E AUDITORIA DE CONFORMIDADE EM SEGURANÇA DA INFORMAÇÃO

Art. 10 A seguir, a matriz com a aplicação do Ciclo PDCA para os processos de gestão de conformidade e auditoria de conformidade em segurança da informação:

Etapa	Gestão de Conformidade	Auditoria de Conformidade
Planejar (P)	Definir políticas, controles e metas de conformidade.	Planejar a auditoria, incluindo o escopo e a metodologia.
Fazer (D)	Implementar controles de segurança e realizar treinamentos.	Realizar a auditoria, coletando dados e realizando entrevistas.
Verificar (C)	Monitorar o desempenho dos controles de segurança.	Analisar os resultados da auditoria e comparar com as normas.
Agir (A)	Ajustar processos, atualizar políticas e corrigir falhas.	Elaborar relatórios de auditoria e recomendar melhorias.

10. RESPONSABILIDADES

Art. 11 Os processos de gestão e auditoria de conformidade em segurança da informação envolvem os seguintes atores e suas respectivas responsabilidades:

I - Alta Administração:

a) Assegurar o alinhamento estratégico e fornecer os recursos necessários para a implementação das ações de segurança da informação;

b) Aprovar diretrizes e políticas de conformidade em segurança da informação;

c) Acompanhar os relatórios de auditoria e assegurar a implementação de melhorias.

II - Gestor de Segurança da Informação:

a) Coordenar a avaliação de conformidade nos aspectos relativos à segurança da informação;

b) Supervisionar a implementação dos controles de segurança;

c) Assegurar a aplicação de ações corretivas e preventivas;

d) Designar, dentre os servidores efetivos do órgão, um ou mais agentes responsáveis pela avaliação de conformidade em segurança da informação.

III - Agente(s) responsável(is) pela avaliação de conformidade em segurança da informação:

a) Implementar e monitorar os controles de segurança;

b) Realizar auditorias internas e avaliações contínuas em segurança da informação;

c) Ministrar treinamentos e conscientizações sobre segurança da informação;

d) Gerenciar a resposta a incidentes de segurança.

IV - Colaboradores e Parceiros:

a) Cumprir as políticas de segurança estabelecidas;

b) Participar dos treinamentos oferecidos;

c) Reportar quaisquer inconformidades ou incidentes de segurança.

11. MATRIZ DE RESPONSABILIDADES (RACI)

Art. 12 A seguir, a matriz RACI dos processos de gestão e auditoria de conformidade em segurança da informação:

Atividade	Alta Administração	Gestor de Segurança	Agente(s) Responsável(is)	Colaboradores e Parceiros
Definição da Estratégia	A	R	C	I
Implementação dos Controles	A	C	R	I
Auditoria e Monitoramento	A	R	R	I
Treinamento Contínuo	A	R	R	I
Resposta a Incidentes	A	R	R	I

(R) Responsável – executa a tarefa;

(A) Aprovador – toma a decisão final;

(C) Consultado – fornece informações;

(I) Informado – acompanha o andamento.

12. INDICADORES DE DESEMPENHO (KPIS)

Art. 13 Para avaliar a efetividade desta norma, serão monitorados os seguintes indicadores de desempenho:

I - % de conformidade nas auditorias internas;

II - Tempo médio de resposta a incidentes;

III - % de colaboradores treinados dentro do prazo;

IV - Número de reincidências por usuário/departamento.

13. PENALIDADES

Art. 14 O descumprimento desta norma poderá resultar em penalidades administrativas, incluindo advertências e sanções disciplinares, conforme as políticas internas.

14. DISPOSIÇÕES FINAIS

Art. 15 Esta norma entra em vigor na data de sua publicação.

Art. 16 As revisões deverão ser periódicas para assegurar a conformidade com melhores práticas e legislações aplicáveis.

Documento assinado eletronicamente por **Gustavo Henrique de Souto Silva**, **Subsecretário de Planejamento e Tecnologia da Informação**, em 30/05/2025, às 18:40, 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 **12636732** e o código CRC **F35BC719**.