PORTARIA MCOM Nº 5983, DE 20 DE JUNHO DE 2022

Aprova a Norma Complementar para Gestão de Riscos de Segurança da Informação.

A GESTORA DE SEGURANÇA DA INFORMAÇÃO, no uso das atribuições que lhe confere o inciso XII, do art. 2º, da Portaria nº 67/SEI-MCOM, de 4 de março de 2021, e tendo em vista o disposto no art. 15, inciso III, do Decreto nº 9.637, de 26 de dezembro de 2018, a Portaria MCOM Nº 2.454, de 22 de abril de 2021, a Resolução CTIR nº 1/2021-SEI-MCTIC, de 3 de dezembro de 2021, os arts. 10, 15 e 19, da Instrução Normativa nº 1, de 27 de maio de 2020, e a Instrução Normativa nº 05, de 30 de agosto de 2021, ambas do Gabinete de Segurança institucional da Presidência da República, resolve:

Art. 1º Aprovar a Norma Complementar para Gestão de Riscos de Segurança da Informação.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

WANESSA QUEIROZ DE SOUZA OLIVEIRA
Gestora de Segurança da Informação

NORMA COMPLEMENTAR PARA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO.

OBJETIVO

Esta norma tem por objetivo estabelecer as diretrizes e procedimentos para gestão de riscos de segurança da informação no âmbito do Ministério das Comunicações - MCOM.

APLICAÇÃO

Os termos definidos nesta norma aplicam-se a todos os agentes públicos do Ministério das Comunicações.

REFERÊNCIA LEGAL E NORMATIVA

Decreto nº 9.203, de 22 de novembro de 2017, que dispõe sobre a política de governança da administração pública federal direta e autárquica e fundacional.

Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

Instrução Normativa nº 2, de 24 de julho de 2020, altera a Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

Portaria GSI/PR nº 93, de 18 de outubro de 2021, que aprova o glossário de segurança da informação;

Portaria MCOM Nº 2.454, de 22 de abril de 2021, que aprova a Política de Segurança da Informação do Ministério das Comunicações;

Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.

Resolução CTIR nº 1/2021-SEI-MCTIC, de 3 de dezembro de 2021, que dispõe sobre a Política de Gestão de Riscos e Controle Interno do Ministério das Comunicações

1. DISPOSIÇÕES GERAIS

1.1 O processo de gestão de riscos de segurança da informação tem por objetivo direcionar e controlar o risco de segurança da informação, a fim de adequá-lo aos níveis aceitáveis para o Ministério.

1.2 O processo de gestão de riscos de segurança da informação é oriundo da Metodologia de Gestão de Riscos do MCOM, que descreve detalhadamente o processo e elenca os documentos utilizados na condução com o objetivo de orientar as unidades a implementá-la em conformidade com o Plano de Integridade e Gestão de Riscos.

1.3 Para fins desta Norma Complementar, serão considerados os conceitos constantes da Metodologia de Gestão de Riscos do MCOM, bem como do Glossário de Segurança da Informação, aprovado e atualizado por portaria do Gabinete de Segurança Institucional da Presidência da República.

1.4 São instâncias de lideranças e gestão de risco de segurança da informação do MCOM:

Nível	Instância	Composição
Estratégico	Comitê de Segurança da Informação (COSIC)	Representantes das unidades: I - Secretaria-Executiva; II - Secretaria de Radiodifusão; III - Secretaria de Telecomunicações; IV - Secretaria Especial de Comunicação Social; V - Gestor de Segurança da Informação do Ministério; VI - Subsecretaria de Planejamento e Tecnologia da Informação; e VII - Coordenação-Geral de Tecnologia da Informação.
Estratégico	Gestor de Segurança da Informação	Gestor de Segurança da Informação, indicado pela Secretaria-Executiva
Tático	Núcleo de Gestão de Riscos de Segurança da Informação (NGRSI)	Gestor de Segurança da Informação, Agente Responsável pela Gestão de Riscos de Segurança da Informação e servidores designados no âmbito da Secretaria-Executiva (apoio às UGRSIs e GPRSIs)
Operacional	Unidades Gestoras de Riscos de segurança da informação (UGRSI)	Responsáveis pelo gerenciamento da gestão de riscos de segurança da informação no âmbito das Unidades do Ministério (composta pelo dirigente máximo e servidores por ele indicados)
Operacional	Gestores de Processos de Riscos de Segurança da Informação (GPRSI)	Responsáveis pela avalição dos riscos no âmbito da sua unidade
Operacional	Servidores	Responsáveis pela operacionalização dos controles internos da gestão

1.5. São atribuições do Núcleo de Gestão de Riscos de Segurança da Informação (NGRSI):

a) fornecer suporte metodológico às unidades gestoras de riscos de segurança da informação;

b) apoiar a elaboração do plano de gestão de riscos de segurança da informação;

c) apoiar a elaboração do relatório de identificação, análise e avaliação dos riscos de segurança da informação; e

d) apoiar a elaboração do relatório de tratamento de riscos de segurança da informação.

1.6. Ao Gestor de Segurança da Informação compete:

a) coordenar o processo de gestão de riscos de segurança da informação;

b) designar o agente responsável pela gestão de riscos de segurança da informação, dentre os servidores efetivos do órgão; e

c) propor medidas preventivas à alta administração.

1.7. São atribuições das Unidades Gestoras de Risco de Segurança da Informação (UGRSI):

a) elaborar o plano de gestão de riscos de segurança da informação;

b) elaborar o relatório de identificação, análise e avaliação dos riscos de segurança da informação; e

c) elaborar o relatório de tratamento de riscos de segurança da informação.

1.7.1 As Unidades Gestoras de Risco de Segurança da Informação (UGRSI) poderão contar com apoio de equipe especializada na execução das atividades de gerenciamento de riscos de segurança da informação.

1.8. São atribuições dos dirigentes das Unidades Gestoras de Riscos de Segurança da Informação (UGRSI):

a) aprovar o plano de gestão de riscos de segurança da informação;

b) aprovar o relatório de identificação, análise e avaliação dos riscos de segurança da informação e encaminhá-lo à alta administração;

c) aprovar o relatório de tratamento de riscos de segurança da informação; e

1.9. Dentro do escopo de um processo de gerenciamento de riscos, deve ser observada a Matriz de Responsabilidade RACI apresentada abaixo:

Atividade	COSIC	Gestor de Segurança / NGRSI	Dirigente	UGRSI	GPRSI
Estabelecimento de limites de exposição a riscos de SI do órgão	R	C	I	I	I
Definição de temas e macroprocessos para gerenciamento de riscos de SI	R	C	I	I	I
Definição do Plano Setorial de Gestão de Riscos de SI	I	C	A	R	C
Estabelecimento do contexto específico	I	C	I	C	R

Identificação de riscos de SI	I	I	I	C	R
Análise de riscos de SI	I	I	I	C	R
Avaliação de riscos de SI	I	I	I	C	R
Tratamento de riscos de SI	I	I	I	C	R
Elaboração do Plano de Tratamentos de Riscos de SI	I	I	A	C	R
Monitoramento e análise crítica	I	I	I	R	R
Comunicação e consulta	I	C / I	I	C / I	C / R
Registro e relato	I	I	I	R	R
Supervisão de riscos chave	A	R	I	C	C

R – Responsável; A – Aprovador; C – Consultado; I - Informado

1.9.1. A Matriz de Responsabilidade RACI define Responsável, Autoridade, Consultado e Informado para o processo de gerenciamento de riscos no MCOM. São elementos da Matriz RACI:

a) Responsável: quem executa a atividade;

b) Autoridade: quem aprova a tarefa ou produto. Pode delegar a função, mas mantém a responsabilidade;

c) Consultado: quem pode agregar valor ou é essencial para a implementação;

d) Informado: quem deve ser notificado de resultados ou ações tomadas, mas não precisa se envolver na decisão.

1.10. Esta Norma Complementar será revisada de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de dois anos.

2. PROCEDIMENTOS

2.1. Processo de Gestão de Riscos de Segurança da Informação

2.1.1 O processo de gestão de riscos de segurança da informação deve ser contínuo, com a execução de suas atividades cíclicas e periódicas, em conformidade com o escopo definido para cada ciclo.

2.1.2 O processo é composto pelas seguintes etapas:

a) estabelecer contexto;

b) identificação de riscos;

c) análise de riscos;

d) avaliação de riscos;

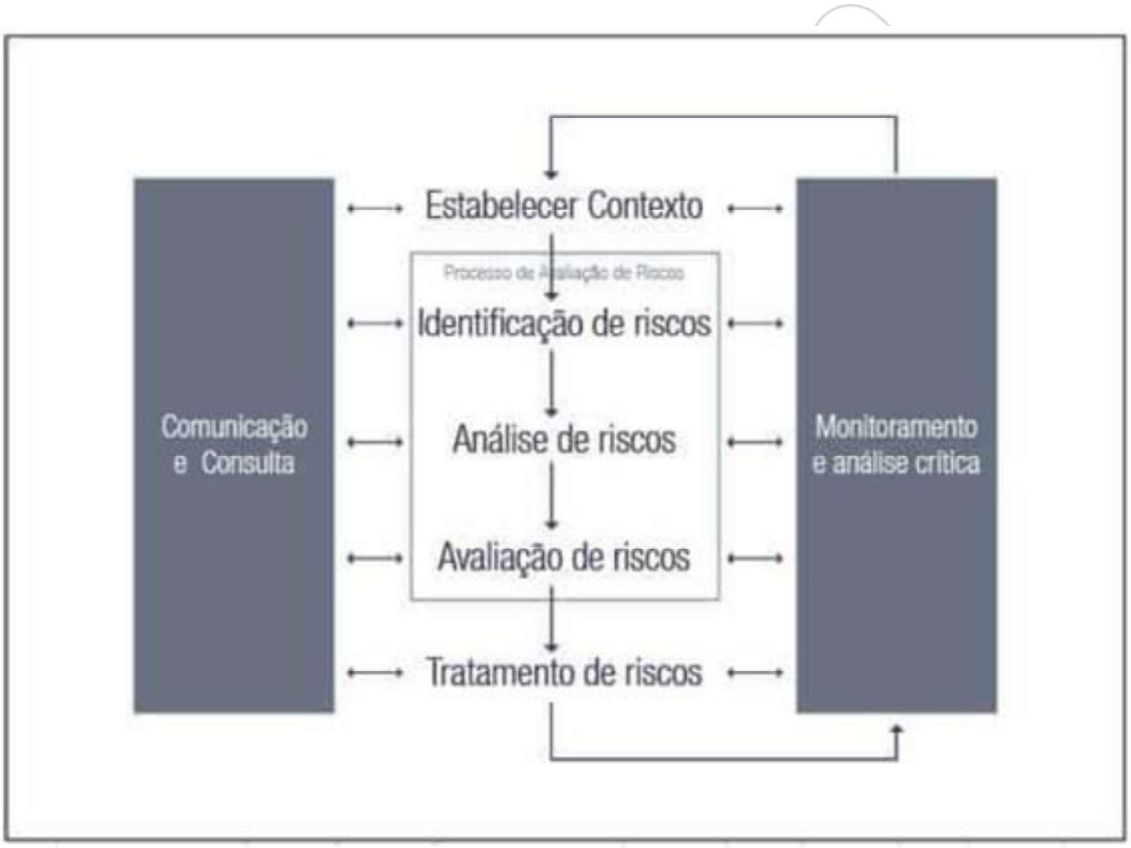
e) tratamento de riscos;

f) comunicação e consulta; e

g) monitoramento e análise crítica.

2.1.3 O detalhamento de cada etapa do processo pode ser encontrado na Metodologia de Gestão de Riscos do MCOM.

2.1.4 Abaixo, segue figura com a representação gráfica do processo de gestão de riscos de segurança da informação.



Fonte: Metodologia de Gestão de Riscos do MCOM

2.1.5 O processo de gestão de riscos de segurança da informação deverá fornecer os seguintes documentos:

a) plano de gestão de riscos de segurança da informação;

b) relatório de identificação, análise e avaliação dos riscos de segurança da informação; e

c) relatório de tratamento de riscos de segurança da informação.

2.2. Plano de Gestão de Riscos de Segurança da Informação

2.2.1. O plano de gestão de riscos de segurança da informação deverá conter, no mínimo:

a) a abrangência da aplicação da gestão de riscos, delimitando seu âmbito de atuação e os ativos de informação que serão objeto de tratamento;

b) a metodologia a ser utilizada que deverá contemplar, no mínimo, critérios de avaliação e de aceitação de riscos;

c) os tipos de riscos;

d) o nível de severidade dos riscos;

e) um modelo do relatório de identificação, análise e avaliação dos riscos de segurança da informação com as orientações necessárias para sua elaboração; e

f) um modelo do relatório de tratamento de riscos de segurança da informação com as orientações necessárias para sua elaboração.

2.2.2. O plano de gestão de riscos da segurança da informação deve ser regularmente revisado, a fim de manter atualizados os riscos relativos aos ativos de informação.

2.2.3. O processo de implementação do plano de gestão de riscos de segurança da informação deverá considerar, dentre outros aspectos, as recomendações de mudanças em relação aos critérios de aceitação de riscos, a abrangência da atuação do plano, as ações de segurança da informação e as atividades de tratamento de riscos previstas.

2.3. Relatório de identificação, análise e avaliação dos riscos de segurança da informação

2.3.1. O relatório de identificação, análise e avaliação dos riscos de segurança da informação deverá ser elaborado com base no modelo estabelecido pelo plano de gestão de riscos de segurança da informação e deverá conter, no mínimo:

a) os riscos associados a cada ativo de informação, considerando as ameaças envolvidas, as vulnerabilidades existentes e as ações de segurança das informações já implementadas;

b) o grau de severidade dos riscos identificados, considerando os valores ou os níveis de probabilidade de ocorrência do risco e as consequências da ocorrência do risco (perda da integridade, disponibilidade, confiabilidade ou autenticidade nos ativos envolvidos);

c) os eventos de segurança da informação ocorridos, com a descrição das ações de segurança, e de eventuais consequências do evento para o órgão ou a entidade;

d) as alterações nos fatores de risco; e

e) as mudanças em relação a critérios de avaliação e análise.

2.3.2. O relatório de identificação, análise e avaliação dos riscos de segurança da informação deverá ser atualizado anualmente e sempre que houver alteração em algum dos fatores de risco ou em algum contexto interno ou externo, devendo ser posteriormente enviado ao gestor de segurança da informação para aprovação.

2.3.3. Entende-se como contextos interno e externo o conjunto de eventos que possam influenciar a capacidade da organização de atingir seus objetivos estratégicos.

2.4. Relatório de tratamento de riscos de segurança da informação

2.4.1. O relatório de tratamento de riscos de segurança da informação deve ser resultante do relatório de identificação, análise e avaliação dos riscos de segurança da informação.

2.4.2. O relatório de tratamento de riscos de segurança da informação deve considerar as possibilidades de tratamento para cada risco identificado.

2.4.3. Para cada possibilidade de tratamento detectada em função do risco identificado, devem ser observados, no que couber:

a) a eficácia das ações de segurança da informação;

b) as restrições técnicas;

c) as restrições físicas estruturais;

d) as restrições operacionais;

e) as restrições organizacionais;

f) os requisitos legais; e

g) a relação custo-benefício.

2.4.4. O relatório de tratamento de riscos de segurança da informação deverá ser elaborado com base no modelo estabelecido pelo plano de gestão de riscos de segurança da informação e deverá conter, no mínimo:

a) a definição e a priorização das ações de segurança e as atividades de tratamento de riscos que deverão ser realizadas;

b) os responsáveis pela execução e pelo acompanhamento das ações de segurança e atividades de tratamento de riscos;

c) os prazos de execução das ações de segurança e das atividades de tratamento de riscos; e

d) as opções de tratamentos de riscos priorizados.