



**MINISTÉRIO DAS COMUNICAÇÕES**  
Secretaria-Executiva do Ministério das Comunicações  
Gabinete da Secretaria-Executiva  
**RESOLUÇÃO N° 26/2024/MCOM**

Brasília, 04 de abril de 2024.

Aprova a Norma Complementar para gestão de mudanças de segurança da informação

O COMITÊ DE GOVERNANÇA DIGITAL, SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS (CGSP), representado por seu presidente conforme designado na Portaria MCOM n° 8.490, de 24 de fevereiro de 2023, Art. 46, e considerando as disposições do art. 49, inciso III, Parágrafo único, da referida Portaria MCOM n° 8.490, de 24 de fevereiro de 2023, resolve:

Aprovar a Norma Complementar para gestão de mudanças de segurança da informação.

Esta Resolução entra em vigor na data de sua publicação.

**JOÃO ALOISIO VIEIRA**  
Secretário-Executivo Adjunto  
Presidente do Comitê de Governança Digital, Segurança da Informação e Proteção de Dados Pessoais

**NORMA COMPLEMENTAR PARA GESTÃO DE MUDANÇAS DE SEGURANÇA DA INFORMAÇÃO**

**OBJETIVO**

Esta norma tem por objetivo estabelecer as diretrizes e procedimentos para a gestão de mudanças 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**

Instrução Normativa GSI/PR N° 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;

Norma Complementar n° 05/IN01/DSIC/GSIPR, e seu anexo - Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU n° 156, de 17 Ago 2009 - Seção 1);

Norma Complementar nº 08/IN01/DSIC/GSIPR - Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU nº 162, de 24 Ago 2010 - Seção 1);

ABNT NBR ISO/IEC 27001:2022 - Segurança da Informação, segurança cibernética e proteção da vida privada - Sistemas de gestão da segurança da informação - Requisitos; e

ABNT NBR ISO/IEC 27002:2022 - Segurança da informação, segurança cibernética e proteção da privacidade — Controles de segurança da informação.

## 1. RESPONSABILIDADES

Art. 1º. Cabe ao gestor de segurança da informação, com relação ao processo de gestão de mudanças nos aspectos de segurança da informação:

- I. Coordenar a gestão de mudanças;
- II. Designar o agente responsável pela gestão de mudança, dentre os servidores efetivos do órgão;
- III. Analisar e encaminhar o documento de avaliação e aprovação de mudança para apreciação da alta administração do órgão, à qual cabe a decisão de aprovar ou indeferir a mudança; e
- IV. Proporcionar a interação constante entre as equipes de gestão de mudanças em aspectos de segurança da informação, de gestão de riscos de segurança da informação e de gestão de continuidade de negócios em segurança da informação.

Art. 2º. Cabe ao agente responsável pela gestão de mudança nos aspectos de segurança da informação:

- I. Recomendar à alta administração a instituição de um grupo técnico de mudança, composto por servidores das áreas afetadas e da área de segurança da informação para a elaboração do documento de avaliação e aprovação de mudança;
- II. Elaborar, juntamente com o grupo técnico de mudança, o documento de avaliação e aprovação de mudança e submetê-lo à análise do gestor de segurança da informação;
- III. Acompanhar, juntamente com o grupo técnico de mudança, os testes da mudança aprovada pelo documento de avaliação e aprovação de mudança;
- IV. Acompanhar, juntamente com o grupo técnico de mudança, a implementação da solução aprovada no documento de avaliação e aprovação de mudança;
- V. Assegurar, juntamente com o grupo técnico de mudança, registro de auditoria contendo todas as informações relevantes relacionadas com a mudança; e
- VI. Informar ao gestor de segurança da informação sobre o andamento e a conclusão do processo.

Art. 3º. Dentro do escopo de um processo de gerenciamento de mudanças, deve ser observada a Matriz de Responsabilidade RACI apresentada abaixo:

| <b>Atividade</b>               | <b>Técnico responsável pela mudança</b> | <b>Agente responsável pela gestão de mudanças</b> | <b>Gestor de segurança da informação</b> |
|--------------------------------|---|---|--|
| Coordenar a gestão de mudanças | I                                       | C/A   | R  |
| Designar o agente responsável  | I                                       | I   | R/A                                      |

|  |     |     |     |
|--|-----|-----|-----|
| Encaminhar o documento de avaliação e aprovação de mudança à alta gestão do Órgão, a fim de obter aprovação ou indeferimento | I   | C   | R/A |
| Avaliar a solicitação de mudança   | I   | R   | A   |
| Avaliar riscos da mudança  | C   | R/A | C   |
| Planejar mudança   | C   | R/A | C   |
| Planejar cronograma  | C   | R/A | C   |
| Planejar plano de comunicação  | C   | R/A | C   |
| Planejar rollback  | C   | R/A | C   |
| Comunicar mudança ao agente responsável  | R/A | I   | I   |
| Comunicar mudança ao gestor de segurança da informação   | I   | R/A | I   |
| Executar mudança   | A   | R   | I   |
| Testar mudança   | A   | R   | I   |
| Executar rollback  | A   | R   | I   |
| Revisão  | A   | R   | I   |

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

I. A Matriz de Responsabilidade RACI define Responsável, Autoridade, Consultado e Informado para o processo de gerenciamento de mudanças de segurança da informação 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; e
- d) Informado: quem deve ser notificado de resultados ou ações tomadas, mas não precisa se envolver na decisão.

## 2. DISPOSIÇÕES GERAIS

Art. 4º. O processo de gestão de mudanças nos aspectos de segurança da informação deve ser respaldado pelas informações levantadas no relatório de identificação, análise e avaliação de riscos de segurança da informação e no relatório de tratamento de riscos de segurança da informação.

## 3. PROCEDIMENTOS

Art. 5º. Para o MCOM, foram adotadas três classificações para mudanças:

- I. Emergencial: mudança não prevista de alto impacto e que ocorre, geralmente, em função de:
  - a) Incidente grave ou modificação nos fatores de risco com alto impacto para os processos da organização;
  - b) Alteração normativa de aplicação imediata;
  - c) Necessidade de modificação significativa imediata nos ativos de informação; e

d) Outros eventos similares.

II. Rotineira: mudança em que a equipe técnica já possui elevado grau de conhecimento e discernimento necessário para realizar a atividade e que ocorre, geralmente, em função de:

a) Atualização da infraestrutura de tecnologia da informação;

b) Serviços de tecnologia da informação com periodicidade habitual que impliquem mudanças de um ou mais aspectos de segurança; e

c) Outros eventos similares.

III. Proativa: mudança em que se busca trazer maior eficiência para a organização e que ocorre geralmente em função de:

a) Ampliação do parque computacional;

b) Obsolescência prevista de equipamentos e processos;

c) Necessidade de adoção de novas tecnologias; e

d) Outros eventos similares.

Art. 6º. O processo de gestão de mudanças deve ser constituído, no mínimo, pelos seguintes instrumentos:

I. Documento de descrição de mudança; e

II. Documento de avaliação e aprovação de mudança.

Art. 7º. O documento de descrição de mudança [Anexo A] tem o objetivo de identificar o tipo de alteração pretendida, de forma a adequar a organização às transformações nos contextos interno e externo.

Art. 8º. Os titulares das unidades demandantes da mudança são responsáveis pela elaboração e aprovação do documento de descrição de mudança, o qual deverá ser remetido ao agente responsável pela gestão de mudanças nos aspectos de segurança da informação.

Art. 9º. O documento de descrição de mudança deverá contemplar pelo menos as seguintes informações:

I. Agente demandante;

II. Unidade de origem;

III. Descrição da mudança;

IV. Tipo de mudança;

V. Objetivo(s) da mudança com os fatores que levaram a esta necessidade; e

VI. Benefícios esperados.

Art. 10. O documento de avaliação e aprovação de mudança [Anexo A] tem o objetivo de:

I. Analisar as mudanças demandadas;

II. Recomendar quais mudanças devem ser aprovadas; e

III. Sugerir as alternativas para a implementação das mudanças.

Art. 11. O documento de avaliação e aprovação de mudança deverá conter, no mínimo:

I. Alternativas para implementação da mudança, com a descrição básica dos procedimentos necessários para sua execução;

- II. Recomendações, em ordem de prioridade, das alternativas a serem adotadas;
- III. Relação entre a mudança pretendida e outras alterações que, eventualmente, possam ocorrer simultaneamente;
- IV. Análise de risco dos ativos de informação que serão afetados pela mudança;
- V. Avaliação do impacto do adiamento da realização da mudança;
- VI. Definição da alternativa a ser implementada ou indeferimento da mudança proposta pela alta administração do órgão ou da entidade; e
- VII. Análise crítica das consequências de mudanças não previstas e de ações propostas para mitigação das eventuais consequências negativas.

Art. 12. Deve-se avaliar também as opções de reversão (rollback) para as mudanças a serem executadas.

Art. 13. Caso necessário, outras instâncias, como a Unidade responsável pela gestão da segurança da informação, também poderão ser consultadas.

Art. 14. Caso o documento de avaliação e aprovação de mudança não tenha sido aprovado e não haja possibilidade de executar a mudança solicitada, a solicitação deve ser encerrada.

Art. 15. Se a mudança se referir a sistemas de informação, é necessária a validação da mudança no ambiente de homologação.

Art. 16. A mudança deverá ser executada no ambiente de homologação, os requisitos de segurança da informação testados e, caso seja uma mudança Emergencial ou uma mudança complexa, a análise de vulnerabilidade realizada por ferramenta específica para essa finalidade.

Art. 17. Caso sejam identificados problemas de segurança / vulnerabilidades, eles deverão ser corrigidos antes da execução no ambiente de produção.

#### 4. EXECUTANDO A MUDANÇA

Art. 18. Na atividade de execução da mudança, o técnico responsável pelo plano de mudança irá executar toda mudança conforme instruções definidas no documento de avaliação e aprovação de mudança.

Art. 19. Caso a mudança tenha sido bem-sucedida e esteja relacionada com um problema, o agente responsável deverá ser notificado para que o registro do problema seja atualizado.

Art. 20. Caso a mudança não tenha sido bem-sucedida, seja por uma falha na execução seja por não ter alcançado o resultado esperado, o técnico responsável pelo plano de mudança deverá Executar Reversão.

Art. 21. Após execução do plano de mudança, bem-sucedida ou não, o técnico responsável pelo plano de mudança deverá informar ao agente responsável e atualizar o plano de mudança, garantindo que todos os registros da execução foram documentados.

#### Anexo A – Documento de descrição, avaliação e aprovação da mudança

| <b>MINISTÉRIO DAS COMUNICAÇÕES</b><br><b>SUBSECRETARIA DE PLANEJAMENTO E TECNOLOGIA DA INFORMAÇÃO</b><br><u>&lt;Nome da Área Solicitante&gt;</u> |              |   |
|--|--------------|---|
| CÓDIGO DO REGISTRO   | DATA         | TIPO DA MUDANÇA                                     |
|  | [dd/mm/aaaa] | [ ] 1. Emergencial [ ] 2. Rotineira [ ] 3. Proativa |

|  |   |   |
|--|---|---|
| <b>ASSUNTO</b>   | Solicitação de Mudança  |   |
| <b>A SER PREENCHIDO PELA ÁREA SOLICITANTE DA MUDANÇA</b> |   |   |
| <b>Unidade de origem da demanda:</b>                     | <i>[Nome da unidade que solicita a mudança]</i>                         |   |
| <b>Agente demandante:</b>                                | <i>[Nome da pessoa que solicitou a mudança]</i>                         |   |
| <b>Telefone/e-mail:</b>                                  | <i>[Telefone e e-mail do solicitante da mudança]</i>                    |   |
| <b>Serviço de TIC:</b>                                   | <i>[Serviço de TIC que sofrerá a mudança]</i>                           |   |
| <b>1</b>   | <b>Esta mudança é resultado de uma ação de gerenciamento de riscos?</b> |   |
|  | <i>Não [ ]</i>  | <i>Sim [ ]</i> <i>ID do Risco: [ ]</i>                          |
| <b>2</b>   | <b>Descrição da mudança</b>   |   |
|  | <i>[Descrever a mudança solicitada]</i>                                 |   |
| <b>3</b>   | <b>Objetivo(s) para a mudança</b>                                       |   |
|  | <i>[Descrever os objetivos para a mudança]</i>                          |   |
| <b>4</b>   | <b>Benefícios esperados</b>   |   |
|  | <i>[Descrever os benefícios esperados com a conclusão da mudança]</i>   |   |
|  | <b>Aprovado/Rejeitado por:</b>  | <i>[Assinatura do Gestor da Unidade Solicitante da mudança]</i> |
|  | <b>Data da aprovação/rejeição:</b>                                      | <i>[dd/mm/aaaa]</i>   |
|  | <b>Comentários:</b>   | <i>[Comentários sobre a mudança solicitada]</i>                 |

|  |  |
|--|--|
| <b>Área executora da mudança:</b>        | <i>[Nome da Área de TI que irá executar a mudança]</i> |
| <b>Responsável pelo preenchimento:</b>   | <i>[Nome da pessoa que irá preencher o documento]</i>  |
| <b>Telefone/e-mail:</b>                  | <i>[Contatos do responsável pelo preenchimento]</i>    |
| <b>Responsável técnico pela mudança:</b> | <i>[Nome da pessoa que irá executar a mudança]</i>     |

|  |  |
|--|--|
| <b>A SER PREENCHIDO PELA ÁREA EXECUTORA DA MUDANÇA</b> |  |
| <i>[após a aprovação da solicitação da mudança]</i>    |  |
| <b>1</b>   | <b>Alternativas para a implementação da mudança</b>  |
|  | <i>[Descrever os procedimentos necessários para a execução da mudança]</i>   |
| <b>2</b>   | <b>Recomendações a serem adotadas</b>  |
|  | <i>[Descrever em ordem de prioridade as alternativas que serão adotadas]</i>   |
| <b>3</b>   | <b>Relação entre a mudança pretendida e outras alterações</b>  |
|  | <i>[Descrever a relação entre a mudança pretendida e outras alterações que, eventualmente, possam ocorrer simultaneamente]</i> |
| <b>4</b>   | <b>Análise de risco dos ativos de informação afetados na mudança</b>   |
|  | <i>[Descrever a análise de risco dos ativos de informação que serão afetados pela mudança]</i>                                 |
| <b>5</b>   | <b>Avaliação do impacto do adiamento da realização da mudança</b>  |
|  | <i>[Descrever os possíveis impactos do adiamento da realização da mudança]</i>   |
| <b>6</b>   | <b>Análise crítica das consequências de mudanças não previstas</b>   |
|  | <i>[Descrever a análise crítica das possíveis consequências de mudanças não previstas]</i>                                     |

|   |  |
|---|--|
| <b>7</b>  | <b>Ações propostas para mitigação das eventuais consequências negativas de mudanças não previstas</b>                    |
| [Descrever as ações propostas para mitigação das eventuais consequências negativas de mudanças não previstas]   |  |
| <b>8</b>  | <b>Cronograma para a execução</b>  |
| [Indicar o cronograma para a execução ou o hiperlink para o documento do cronograma, preparado em conjunto com a área solicitante e as outras áreas envolvidas] |  |
| <b>9</b>  | <b>Itens de configuração envolvidos na mudança</b>   |
| [Descrever os itens de configuração que serão utilizados durante a mudança]   |  |
| <b>10</b>   | <b>Risco da mudança</b>  |
| [Avaliar o risco envolvido na implantação da mudança]   |  |
| [ ] 1. Baixo [ ] 2. Médio [ ] 3. Alto   |  |
| <b>11</b>   | <b>Plano de comunicação da mudança</b>   |
| [Descrever o plano de comunicação da mudança]   |  |
| <b>12</b>   | <b>Plano de retorno (Rollback)</b>   |
| [Descrever o plano de retorno (Rollback)]   |  |
| <b>13</b>   | <b>Definição da alternativa a ser implementada ou indeferimento da mudança proposta pela alta administração do órgão</b> |
| [Descrever a definição da alternativa a ser implementada ou o indeferimento da mudança proposta pela alta administração do órgão]                               |  |
| <b>Aprovado por:</b>  | [Aprovação do Gestor de Segurança da Informação]   |
| <b>Comentários:</b>   | [Comentários sobre a mudança solicitada]   |



Documento assinado eletronicamente por **João Aloísio Vieira, Secretário-Executivo Adjunto**, em 04/04/2024, às 18:25, 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 **11458151** e o código CRC **C6AB5AD5**.