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

# RESOLUÇÃO Nº 31/2025/MCOM de 06 de fevereiro de 2025.

Aprova a Norma Complementar para Gestão de Continuidade de Negócios 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 de Continuidade de Negócios em Segurança da Informação na forma do Anexo I.

Art. 2º Esta Resolução entrará em vigor no primeiro dia útil subsequente ao da 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 DE CONTINUIDADE DE NEGÓCIOS EM SEGURANÇA DA INFORMAÇÃO

### OBJETIVO

O processo de Gestão de Continuidade de Negócios em Segurança da Informação – GCN tem como objetivo principal investigar, desenvolver e implementar opções de recuperação dos serviços de TI, assegurando que o Ministério das Comunicações - MCOM esteja preparado para enfrentar e se recuperar de situações adversas, mantendo seus serviços de TI essenciais em funcionamento e protegendo seus ativos críticos.

### 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 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;

Norma Complementar nº 06/IN01/DSIC/GSIPR - Estabelece as diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

ABNT NBR ISO/IEC 27001:2022 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação – Requisitos; e

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

## CONCEITOS E DEFINIÇÕES

0.1. Para facilitar a compreensão dos termos usados neste processo, seguem as definições de cada conceito:

I - Acesso: ato de ingressar, consultar ou utilizar informações e ativos de informação de um órgão ou entidade, respeitando as restrições de acesso que possam ser aplicáveis.

II - Ameaça: fator externo ou potencial causador de um incidente indesejado, capaz de causar danos a sistemas ou organizações.

III - Análise de impacto nos negócios: processo de estimar os efeitos da interrupção de serviços e cenários de desastre no desempenho de órgãos ou entidades da administração pública federal (APF), avaliando a criticidade dos processos de negócios, prioridades de recuperação, interdependências e requisitos de segurança da informação para alcançar os objetivos de recuperação dentro dos prazos estabelecidos.

IV - Análise de incidentes: exame das informações disponíveis sobre um incidente, incluindo artefatos e evidências, para identificar seu escopo, extensão, natureza e os danos causados. Inclui também a proposição de estratégias de contenção e recuperação.

V - Análise de riscos: uso sistemático de informações para identificar fontes de risco e estimar os riscos.

VI - Atividade: ação ou conjunto de ações realizadas por um órgão ou entidade, que produzem ou suportam produtos ou serviços.

VII - Ativo: qualquer elemento de valor para a organização.

VIII - Ativos de informação: meios de armazenamento, transmissão e processamento de informações, equipamentos associados, sistemas utilizados, locais onde estão situados esses recursos e as pessoas que têm acesso a eles.

IX - Ataque: tentativa intencional e não autorizada de acessar ou manipular informações, tornando um sistema inacessível ou comprometido em sua integridade.

X - Contingência: recursos disponíveis para substituição em caso de falha no ambiente principal, como servidores, computadores, no-breaks e equipamentos de conectividade.

XI - Continuidade de negócios: capacidade de uma organização de se planejar e responder a incidentes e interrupções, reduzindo seus impactos e recuperando ativos críticos para manter operações em níveis aceitáveis.

XII - Desastre: evento súbito e não planejado que causa perda significativa para a organização, afetando seriamente sua capacidade de prestar serviços essenciais ou críticos.

XIII - Disponibilidade: condição de tornar a informação acessível aos usuários sempre que necessário para quaisquer finalidades.

XIV - Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR): grupo responsável por receber, analisar e responder a notificações de incidentes de segurança.

XV - Evento: mudança de estado relevante para a gestão de um serviço de TI, podendo incluir alertas de monitoramento ou uso intensivo de recursos.

XVI - Gestão de continuidade: processo de gestão abrangente que identifica ameaças e seus impactos nas operações, desenvolvendo uma estrutura de resiliência organizacional.

XVII - Gestão de riscos: processo contínuo de identificação, avaliação e gerenciamento de eventos que possam impactar a organização, promovendo segurança razoável para o alcance de objetivos.

XVIII - Gestão de segurança da informação: práticas e métodos que integram gestão de riscos, continuidade de negócios, tratamento de incidentes, conformidade e segurança nos processos institucionais.

XIX - Incidente: interrupção imprevista ou redução de qualidade de um serviço, com impacto na prestação de serviços de TI, como indisponibilidade de acesso ou falha em equipamentos.

XX - Informação: dados que podem ser utilizados para gerar conhecimento e estão contidos em qualquer meio ou formato.

XXI - Interrupção: evento que causa um desvio negativo na entrega de produtos ou serviços, podendo ser previsto ou não.

XXII - Plano de continuidade de negócios: documentação dos procedimentos para que órgãos ou entidades mantenham a continuidade de suas atividades críticas em locais alternativos em casos de incidentes.

XXIII - Risco: possibilidade de um evento afetar o cumprimento dos objetivos da organização, medido em termos de impacto e probabilidade.

XXIV - Risco de segurança da informação: potencial de exploração de vulnerabilidades de ativos de informação, com possível impacto negativo para a organização.

XXV - Segurança da informação: práticas para assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações.

XXVI - Serviços de tecnologia da informação: provisão de serviços de TI, como desenvolvimento, manutenção, armazenamento e operação de sistemas.

XXVII -Sistemas de informação: conjunto de elementos materiais ou intelectuais que permitem a integração de recursos de tecnologia, informação e comunicação.

XXVIII
- Tecnologia da informação: ativo estratégico que apoia os processos de negócios, processando e disseminando informações para os usuários.

XXIX - Usuário: pessoa autorizada para acessar os ativos de informação de um órgão ou entidade da APF.

**PROCEDIMENTOS**

0.2. A Gestão de Continuidade de Negócios em Segurança da Informação (GCN) abrange práticas, estratégias e processos que visam garantir que os serviços de TI atendam às necessidades e aos objetivos do MCOM. Esse processo cobre diversas áreas, incluindo o alinhamento estratégico, gestão de portfólio de serviços, governança de TI, gestão de riscos, relacionamento com clientes, melhoria contínua de processos, medição de desempenho com indicadores-chave, além da gestão financeira, de projetos, mudanças, e inovação tecnológica.

0.3. De acordo com a Information Technology Infrastructure Library (ITIL), o processo de GCN em segurança da informação é focado em apoiar a continuidade dos negócios, assegurando a retomada dos serviços dentro dos prazos definidos em casos de interrupções significativas. Este processo foca no planejamento preventivo, antecipação e gestão de incidentes, visando manter a disponibilidade e o desempenho do serviço em níveis elevados, mesmo em situações de crise.

0.4. O objetivo é que o provedor de serviços de TI esteja preparado para oferecer um nível mínimo de serviço, reduzindo os riscos a um patamar aceitável diante de desastres. Esse processo envolve:

I - estabelecimento de uma política de continuidade de negócios em segurança da informação;

II - definição dos requisitos mínimos necessários para retomada de serviços em casos de interrupções;

III - análise e mitigação de riscos relacionados a desastres em serviços de TI, incluindo transferência de riscos para terceiros, quando adequado;

IV - elaboração de um plano de continuidade de negócios adaptado às necessidades do MCOM;

V - planejamento de estruturas para a retomada dos serviços;

VI - capacitação e conscientização da organização para situações críticas; e

VII - execução de testes, auditorias, controles e gestão de mudanças na estrutura de continuidade.

0.5. O processo de GCN, adotado pela área de TI do MCOM, é estruturado em cinco fases, orientadas pelo ciclo de melhoria contínua PDCA. Essas fases abrangem atividades de iniciação, definição de requisitos e estratégias, implementação, operação e ativação de um plano de GCN em segurança da informação. As fases do processo são apresentadas na tabela a seguir:

| Processo de gestão de continuidade de negócios em segurança da informação | |
|---|---|
| Entrada | Informações sobre os serviços e os níveis de serviço do gerenciamento de catálogo de Serviço e nível de serviço. |
| Fases | 1. Planejamento e iniciação.<br>2. Análise de impacto nos negócios.<br>3. Estratégias de recuperação.<br>4. Desenvolvimento e implementação.<br>5. Manutenção e revisão. |
| Saída | Plano de gestão de continuidade de negócios em segurança da informação. |

0.5.1. **Planejamento e Iniciação**

A etapa de planejamento e iniciação em GCN é essencial para assegurar que o MCOM esteja capacitado a enfrentar e se recuperar de eventos que possam comprometer suas operações. Nessa fase, são estabelecidos os objetivos, metas, processos e procedimentos fundamentais para a GCN. Esse processo abrange a realização das seguintes atividades:

I - entender a organização, reconhecendo a necessidade de continuidade de negócios em segurança da informação;

II - definir o escopo da gestão de continuidade de negócios em segurança da informação;

III - definir os termos de referência de gestão de continuidade de negócios em segurança da informação;

IV - definir as estratégias para a gestão de continuidade de negócios em segurança da informação;

V - alocar recursos para a gestão de continuidade de negócios em segurança da informação;

VI - definir papéis e responsabilidades para a gestão de continuidade de negócios em segurança da informação; e

VII - estabelecer políticas e objetivos.

0.5.2. **Análise de impacto nos negócios**

A etapa de análise de impacto nos negócios tem como objetivo avaliar os potenciais impactos de interrupções nos processos e operações essenciais do MCOM. Esse estudo oferece insights valiosos para direcionar o desenvolvimento de estratégias de continuidade, garantindo que a instituição concentre seus recursos nas áreas mais críticas para manter suas operações essenciais ativas durante e após uma interrupção.

Essa fase é crucial para definir prioridades, estabelecer metas práticas e elaborar estratégias eficazes de continuidade. As atividades envolvidas nesta fase incluem:

I - identificação e mapeamento dos processos de negócios que são essenciais para o funcionamento do MCOM;

II - classificação dos processos com base em sua importância para as operações globais;

III - análise das relações e dependências entre os diversos processos e sistemas;

IV - identificação de recursos compartilhados e interdependências que podem afetar a continuidade operacional;

V - avaliação do impacto financeiro de interrupções nos processos críticos;

VI - estabelecimento de metas de tempo para a recuperação de processos críticos;

VII - definição de janelas de recuperação aceitáveis para minimizar perdas e interrupções;

VIII - identificação e alocação de recursos humanos, tecnológicos e físicos necessários para a continuidade operacional;

IX - avaliação da disponibilidade e capacidade desses recursos;

X - identificação dos riscos residuais após a implementação de medidas de mitigação;

XI - análise de lacunas entre as capacidades atuais e as necessárias para atender aos objetivos de continuidade;

XII - classificação dos processos críticos e recursos em termos de prioridade para a continuidade;

XIII - fornecimento de informações essenciais para orientar o desenvolvimento de estratégias de recuperação;

XIV - registro de todas as descobertas e decisões durante a análise de impacto nos negócios;

XV - criação de documentação que servirá como base para o desenvolvimento de planos de continuidade; e

XVI - revisão periódica da análise de impacto nos negócios para garantir que esteja alinhada com as mudanças no MCOM, nos processos ou no ambiente de negócios.

**Estratégias de recuperação**

A fase de desenvolvimento de estratégias de recuperação é essencial para criar planos específicos que permitam ao MCOM restabelecer suas operações essenciais após uma interrupção significativa. Essa etapa busca identificar e implementar estratégias eficazes para restaurar as funções críticas do MCOM dentro dos prazos de recuperação definidos.

As atividades dessa fase incluem:

XVII - desenvolvimento de estratégias para mitigar os impactos identificados;

XVIII - estabelecimento de planos de recuperação de desastres e continuidade de negócios em segurança da informação;

XIX - implementação de medidas preventivas e de contingência;

XX - estabelecimento de sequências de ações, responsabilidades e recursos necessários para a recuperação;

XXI - estabelecimento de acordos e planos de ação conjuntos;

XXII - realização de testes regulares e exercícios para validar a eficácia das estratégias de recuperação;

XXIII - identificação de áreas de melhoria e ajustes nos planos com base nos resultados dos testes;

XXIV - desenvolvimento de procedimentos claros de comunicação para garantir uma resposta rápida e coordenada durante a implementação das estratégias de recuperação;

XXV - estabelecimento de canais de comunicação eficazes com partes interessadas internas e externas; e

XXVI - treinamento regular da equipe responsável pela execução das estratégias de recuperação.

**Desenvolvimento e implementação**

A fase de desenvolvimento e implementação é crucial para assegurar a resiliência do MCOM diante de eventos inesperados. Nessa etapa, são colocados em prática os planos, agendas de testes, relatórios, controles, processos e procedimentos necessários. As atividades envolvidas incluem:

XXVII -elaboração do plano detalhado de continuidade de negócios em segurança da informação;

XXVIII
- treinamento de servidores e partes interessadas;

XXIX - desenvolvimento de estratégias para mitigar os riscos e garantir a continuidade das operações;

XXX - formação de uma equipe responsável pela implementação e manutenção do plano de continuidade de negócios;

XXXI - documentação de procedimentos detalhados para a recuperação de sistemas, processos e comunicações;

XXXII -estabelecimento de protocolos de comunicação para informar as partes interessadas internas e externas durante uma interrupção;

XXXIII
- realização de testes regulares do plano para garantir eficácia e fazer ajustes necessários;

XXXIV
- capacitação da equipe responsável pelo plano de continuidade de negócios em segurança da informação;

XXXV -implementação do plano de continuidade de negócios em segurança da informação em uma escala menor para identificar possíveis problemas antes da implementação em todo o MCOM; e

XXXVI
- expansão da implementação do plano de continuidade de negócios em segurança da informação para todos os setores do MCOM, garantindo que todos estejam cientes e preparados para seguir os procedimentos.

0.5.3. **Manutenção e revisão**

Esta fase é encarregada de realizar a manutenção e revisão contínua do processo de continuidade de negócios, além de, quando necessário, avaliar o desempenho em relação às políticas, objetivos e experiências práticas, e reportar os resultados por meio de análises críticas. Também é responsável por avaliar periodicamente o desempenho e a conformidade do processo, promovendo os ajustes necessários. As atividades envolvidas nesta fase incluem:

I - atualização contínua do plano de continuidade de negócios em segurança da informação para refletir mudanças organizacionais, tecnológicas ou de risco;

II - revisão após incidentes reais para identificar melhorias;

III - garantia de conformidade com regulamentos e padrões vigentes;

IV - manutenção e atualização contínua da documentação dos planos de recuperação para refletir mudanças na organização, processos ou ambiente de negócios; e

V - avaliação constante das estratégias de recuperação à medida que a organização evolui, garantindo que estejam alinhadas com as mudanças nas operações e no ambiente de negócios.

## PAPÉIS E RESPONSABILIDADES

0.6. Um papel consiste em um conjunto de responsabilidades, atividades e autoridades claramente definidas dentro de um processo, sendo atribuídas a uma pessoa, equipe ou função específica. Os papéis e responsabilidades estabelecidos no processo de GCN são:

**Subcomitê de Segurança da Informação - SINF**

É responsável pela decisão final sobre o escopo, política e diretrizes sobre a gestão de continuidade de negócios em segurança da informação. Este Subcomitê tem as seguintes responsabilidades referente a GCN:

I - prover a orientação e o apoio necessário às ações de continuidade de negócios, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes;

II - aprovar a estratégia de continuidade de negócios em segurança da informação;

III - aprovar as diretrizes estratégicas que norteiam a elaboração do plano de gestão de

continuidade de negócios em segurança da informação;

IV - disponibilizar os recursos necessários (humanos, tecnológicos e financeiros) para estabelecer, implementar, operar e manter o plano de gestão de continuidade de negócios em segurança da informação.

V - avaliar e aprovar a política, norma interna complementar e processo de gestão de continuidade de negócios em segurança da informação.

**Gestor de Segurança da Informação**

Compete ao Gestor de Segurança da Informação as seguintes responsabilidades referentes a GCN:

VI - elaborar e coordenar o processo de gestão de continuidade de negócios em segurança da informação conjuntamente com a área de TI, considerando os aspectos de segurança da informação;

VII - realizar ajustes no processo de gestão de continuidade de negócio em relação à segurança da informação com a finalidade de estar em conformidade com a legislação vigente no âmbito da administração pública federal; e

VIII - designar um agente responsável pela execução das atividades referentes ao processo de GCN, dentre os servidores efetivos do MCOM.

**Equipe de Tratamento e Resposta de Incidentes Cibernéticos - ETIR**

Equipe responsável pela gestão do processo de continuidade de serviços de TI. Compete à estas pessoas a seguinte responsabilidade:

IX - avaliar a política, norma interna complementar, processo, plano, procedimentos e atividades sobre gestão de continuidade de negócios em segurança da informação.

**Setor de TI (Coordenação-Geral de Tecnologia da Informação e Comunicação e demais setores de TI das unidades do MCOM)**

Agente responsável pela execução das atividades referentes ao processo de GCN. Representado pelo responsável pela área de TI no MCOM. Este papel tem as seguintes responsabilidades:

X - assessorar os responsáveis pelo processo ou os titulares das unidades em que forem identificadas atividades críticas nas atribuições referentes a gestão de continuidade de serviços de TI;

XI - avaliar o plano de continuidade de negócios em segurança da informação e propor mudanças, quando aplicável;

XII - supervisionar a implementação, os testes de funcionamento e a atualização do plano de continuidade de negócios em segurança da informação;

XIII - propor melhorias na implementação de novos controles relativos ao plano de continuidade de negócios em segurança da informação;

XIV - participar da elaboração da análise de impacto nos negócios; e

XV - propor medidas visando ao desenvolvimento da cultura de gestão de continuidade de negócios em segurança da informação.

**Coordenação de Segurança da Informação**

Setor responsável pelo processo em que forem identificadas atividades críticas. Compete a este setor as seguintes responsabilidades:

XVI - propor as diretrizes a serem contempladas no plano de GCN com base em processos de segurança da informação;

XVII - elaborar o plano de continuidade de negócios em segurança da informação;

XVIII - realizar os testes de funcionamento do plano de continuidade de negócios em segurança da informação com base em requisitos de segurança da informação;

XIX - avaliar e aprimorar o plano de continuidade de negócios em segurança da informação a partir dos resultados dos testes de funcionamento;

XX - gerenciar a contingência quando ocorrer a interrupção de atividades, com base no plano de

continuidade de negócios em segurança da informação desenvolvido; e

XXI - propor os recursos necessários para a implementação e o desenvolvimento das ações relacionadas à continuidade das atividades, bem como para a realização dos testes de funcionamento do plano de continuidade de negócios em segurança da informação.

**Usuários**

Pessoas que utilizam os dados e informações processados pelo MCOM. Cabe aos usuários as seguintes responsabilidades:

XXII - utilizar os dados e informações no MCOM prioritariamente para a realização das atividades desempenhadas nos limites da ética, razoabilidade e legalidade;

XXIII - notificar incidentes de segurança da informação; e

XXIV - evitar na medida do possível se envolver em incidentes de segurança da informação.

**MATRIZ RACI**

0.7. A matriz RACI apresentada na tabela a seguir é utilizada para definir com clareza as atribuições, papéis e responsabilidades de cada colaborador nas atividades do processo. A sigla RACI significa, em inglês: responsible, accountable, consulted e informed.

I - responsible (responsável): pessoa, função ou unidade organizacional responsável pela execução de uma atividade no âmbito de um processo;

II - accountable (responsabilizado): dono da atividade, deverá fornecer os meios para que a atividade possa ser executada, e será responsabilizado caso a atividade não alcance os seus objetivos; cada atividade só pode possuir um accountable;

III - consulted (consultado): pessoa que deverá ser consultada durante a execução da atividade; as informações levantadas junto a essas pessoas tornam-se entradas para a execução da atividade;

IV - informed (informado): pessoa que será informada acerca do progresso da execução da atividade.

| Fase | SINF | GSI | ETIR | CGTI | COSEG | U |
|---|---|---|---|---|---|---|
| Planejamento e iniciação | A | C | C | C | R | I |
| Análise de impacto nos negócios | A | C | C | C | R | I |
| Estratégias de Recuperação | A | C | C | C | R | I |
| Desenvolvimento e implementação | A | C | C | C | R | I |
| Manutenção e revisão | A | C | C | C | R | I |

Legenda:
SINF: Subcomitê de Segurança da Informação.
GSI: Gestor de Segurança da Informação.
ETIR: Equipe de Tratamento e Resposta a Incidentes Cibernéticos.
CGTI: (Coordenação-Geral de Tecnologia da Informação e Comunicação e demais setores de TI das unidades do MCOM).
COSEG: Coordenação de Segurança da Informação.
U: Usuários.

**INDICADOR DE DESEMPENHO**

0.8. O processo de GCN será monitorado e avaliado periodicamente por meio de indicadores de desempenho, a fim de realizar os ajustes necessários. O objetivo desse monitoramento é acompanhar a eficácia do processo, identificando tendências, falhas e oportunidades de correção, promovendo assim a melhoria contínua. Para avaliar a eficiência deste processo, foi definida a métrica operacional, detalhada na tabela a seguir:

| | |
|---|---|
| Indicador | Quantidade de serviços de TI contemplados no plano de continuidade de negócio em segurança da informação. |
| Descrição | Número de serviços de TI contemplados no plano de continuidade de negócios em segurança da informação. |
| Objetivo | Aumentar o número de serviços de TI contemplados no plano de continuidade de negócios em segurança da informação. |
| Periodicidade | Anual |
| Fonte | Coordenação-Geral de Tecnologia de Informação e Comunicação |
| Fórmula | Somatório de serviços contemplados no plano de continuidade de negócios em segurança da informação. |
| Meta | Aumentar a quantidade de serviços de TI contemplados no plano de continuidade de negócios em segurança da informação. |

## DISPOSIÇÕES FINAIS

0.9. Os casos omissos ou as dúvidas suscitadas na aplicação desta norma, serão dirimidas pelo SINF, com assessoramento técnico da Subsecretaria de Planejamento e Tecnologia da Informação.

0.10. As propostas de alteração desta norma deverão ser encaminhadas ao SINF.

Documento assinado eletronicamente por **Gustavo Henrique de Souto Silva**, **Subsecretário de Planejamento e Tecnologia da Informação**, em 08/02/2025, às 17:34, 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 **12249693** e o código CRC **BF726EE6**.

**Referência:** Processo nº 53115.016204/2023-36 Documento nº 12249693