Política de Gestão de Continuidade de Negócios

Anexo Único

1ª Edição

Agosto/2026

CONTROLADORIA GERAL

GOV RJ

POLÍTICA DE CONTINUIDADE DE NEGÓCIOS

BRUNO CAMPOS PEREIRA
Controlador-Geral do Estado

DANIELA QUEIROZ ROCHA
Chefe de Gabinete

THIAGO COUTO LAGE
Subcontrolador-Geral do Estado

DÉBORA TAVARES DURSO
Auditora-Geral do Estado

ALLAN COSTA DOS REIS
Corregedor-Geral do Estado

EUGENIO MANUEL DA SILVA MACHADO
Ouvidor-Geral do Estado

Elaborado por:

Comitê Integrado de Governança de Tecnologia e Segurança da Informação da Controladoria Geral do Estado do Rio de Janeiro – CGTI (Resolução CGE nº 395, de 10 de fevereiro de 2026).

POLÍTICA DE CONTINUIDADE DE NEGÓCIOS

COMITÊ INTEGRADO DE GOVERNANÇA DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO

Gabinete da Controladoria Geral do Estado
Thiago Augusto de Azevedo Cavalcante
Suplente: Luiz Flavio Mathias de Mello Moraes

Subcontroladoria Geral do Estado
Letícia Spínola Flávio
Suplente: Suelen Aparecida Rodrigues de Oliveira

Corregedoria Geral do Estado
Camila Alves Ribeiro
Suplente: Beatriz Lage Brum

Auditoria Geral do Estado
Marcus Vinícius dos Santos
Suplente: Daniella Kircher

Ouvidoria e Transparência Geral do Estado
Tiago Nunes Figueiredo
Suplente: Myrla Raianne Ferreira dos Santos

Diretoria Geral de Administração e Finanças
Luiz Augusto Guimarães Silva
Suplente: Patrícia Viçoso Figueiredo

Assessoria de Planejamento e Orçamento
Jorge Pereira da Silva
Maria Victória Silveira de Andrade Cordeiro

Assessoria de Tecnologia da Informação
Claudio José Ascenção de Andrade
Suplente: Roberta da Silva Macedo Mello

Gestor de Segurança da Informação
Daiene dos Santos Costa
Suplente: Renato Mattos Miragaia

Encarregado Setorial pelo Tratamento de Dados Pessoais
Rafael Antônio da Silva Vianna
Suplente: Myrla Raianne Ferreira dos Santos

DOCUMENTO PÚBLICO

Este documento é classificado como público e pode ser acessado e compartilhado livremente, observadas as normas e legislações vigentes. As informações nele contidas destinam-se à divulgação das práticas e diretrizes de gestão de riscos adotadas pelo órgão. Sua reprodução é permitida, desde que preservada a integridade do conteúdo e mencionada a fonte institucional. Alterações que comprometam o significado ou a finalidade das informações são de responsabilidade de seus autores.

CONTROLE DE VERSÃO

Data	Versão	Autor	Alteração	Responsável
13/04/2026	0.1	Controladoria Geral do Estado do Rio de Janeiro	Elaboração da Política de Gestão de Continuidade de Negócios	Comitê Integrado de Governança de Tecnologia e Segurança da Informação da Controladoria Geral do Estado do Rio de Janeiro – CGTI
14/08/2026	1.0	Controladoria Geral do Estado do Rio de Janeiro	Aprovação da Política de Gestão de Continuidade de Negócios	Comitê Integrado de Governança de Tecnologia e Segurança da Informação da Controladoria Geral do Estado do Rio de Janeiro – CGTI

SUMÁRIO

1. APRESENTAÇÃO

O intuito deste documento é estabelecer princípios, diretrizes e responsabilidades para a orientação dos processos de continuidade de negócios incluindo seu planejamento, implementação e operação, avaliação de desempenho, análise crítica e melhoria contínua inerentes às atividades da Controladoria Geral do Estado do Rio de Janeiro (CGE-RJ), incorporando a visão de continuidade operacional ao seu planejamento estratégico e à tomada de decisões, em conformidade com as regulamentações aplicáveis, ou seja, um instrumento normativo formal que estabelece diretrizes, princípios e responsabilidades para assegurar que a CGE-RJ seja capaz de manter ou restabelecer suas operações essenciais em níveis aceitáveis, diante de incidentes disruptivos.

Inserida no contexto da Gestão de Continuidade de Negócios, essa política constitui a base para a implementação de processos sistemáticos voltados à prevenção, resposta e recuperação frente a eventos que possam comprometer a continuidade operacional, tais como desastres naturais, falhas tecnológicas, interrupções de infraestrutura ou incidentes de segurança da informação. Esses aspectos serão tratados operacionalmente no Plano de Recuperação de Desastres (PRD) e no Plano de Continuidade Operacional (PCO).

2. ABRANGÊNCIA

Art. 1° Esta Política aplica-se a todos os servidores, consultores, dirigentes, estagiários, fornecedores, trabalhadores terceirizados, visitantes e demais partes envolvidas que atuem na elaboração, manutenção, execução ou apoio às atividades relacionadas à Gestão de Continuidade de Negócio da CGE-RJ, aplicando-se, também, a processos, serviços e ativos críticos, ambientes corporativos e remotos, além de unidades administrativas, que integrem ou suportem o Sistema de Continuidade de Negócio da CGE-RJ.

3. TERMOS E DEFINIÇÕES

Art. 2° Para os fins desta Política, devem ser observados os seguintes conceitos e definições:

I. **análise de impacto nos negócios:** processo de análise do impacto sobre o tempo de uma disrupção na organização;

II. **atividade:** conjunto de ações realizadas por uma unidade administrativa para a execução de um processo ou serviço;

III. **continuidade de negócios:** capacidade de uma organização de continuar a entrega de produtos e serviços dentro de períodos aceitáveis e com capacidade predefinida durante uma disrupção;

IV. **desastre:** evento inesperado que provoca a interrupção ou indisponibilidade significativa de processos, serviços ou sistemas críticos, exigindo a ativação dos planos de continuidade e recuperação;

V. **disrupção:** um evento que interrompe a normalidade de funções, operações ou processos de forma antecipada ou não;

VI. **evento:** ocorrência ou mudança de circunstâncias que podem levar a uma interrupção, falha ou crise;

VII. **gestão de continuidade de negócios:** processo de implementação e manutenção da continuidade de negócios;

VIII. **impacto:** consequência de uma interrupção ou incidente que afeta os negócios, processos ou operações da organização;

IX. **melhoria contínua:** atividade recorrente realizada para aumentar a performance de um processo ou equivalente;

X. **período máximo tolerável de interrupção (MTPD—*Maximum Tolerable Period of Disruption*):** tempo máximo que levaria para um impacto adverso tornar-se inaceitável. O MTPD é determinado com base na consideração de uma interrupção que ocorre no pior momento possível, bem como o tempo subsequente necessário para resultar em um impacto negativo relevante;

XI. **plano de continuidade operacional (PCO):** documento com procedimentos para a retomada das funções de negócio críticas, garantindo sua continuidade dentro dos tempos aceitáveis;

XII. **Plano de Recuperação de Desastres (PRD):** documento que descreve as ações que devem ser executadas para recuperação dos sistemas de informação de maior criticidade. O plano deve permitir que as operações sejam reestabelecidas após um incidente que impossibilite sua operação;

XIII. **ponto objetivo de recuperação (RPO - Recovery *Point Objective*):** ponto em que as informações utilizadas por uma atividade devem ser restauradas, a fim de permitir que a atividade possa operar após a recuperação;

XIV. **recuperação:** conjunto de ações destinadas a restaurar processos, sistemas ou serviços após uma interrupção;

XV. **recursos:** pessoas, sistemas, infraestrutura, informações ou fornecedores essenciais para a execução do processo;

XVI. **risco:** possibilidade de ocorrência de um evento ou condição que possa causar impacto negativo no alcance dos objetivos institucionais, afetando processos, serviços, recursos ou informações;

XVII. **sistema de gestão de continuidade de negócios (SGCN):** estrutura que estabelece, implementa e mantém a capacidade da instituição em responder as interrupções;

XVIII. **tempo objetivo de recuperação (RTO - Recovery *Time Objective*):** tempo previsto para recuperação de uma função crítica de negócios a um nível aceitável após sua interrupção;

XIX. **unidades administrativas:** áreas organizacionais responsáveis pela execução de processos, atividades e serviços sob sua competência, incluindo gerências, superintendências, coordenações, assessorias e unidades equivalentes.

4. PRINCÍPIOS

Art. 3° Esta Política deve obedecer aos seguintes princípios, além dos previstos na Política de Segurança da Informação (PSI) da CGE-RJ:

I. **disponibilidade dos processos críticos**: garantia de que os processos e serviços essenciais sejam mantidos ou retomados dentro dos prazos e níveis aceitáveis, mesmo em situações de interrupção;

II. **resiliência organizacional**: capacidade de prevenir, responder e recuperar-se de incidentes, minimizando impactos financeiros, operacionais, regulatórios, imagem e políticos;

III. **continuidade orientada a riscos e impactos**: tratamento diferenciado dos processos e recursos com base nos riscos, na criticidade e nos impactos para a CGE-RJ;

IV. **melhoria contínua**: aprimoramento permanente do Sistema de Gestão de Continuidade de Negócios por meio de testes, exercícios, auditorias e lições aprendidas.

5. DIRETRIZES

As seguintes diretrizes são a base do sistema de gestão de continuidade de negócios da CGE-RJ e devem ser adotadas para o alcance dos objetivos desta Política.

Art. 4° A CGE-RJ manterá um Sistema de Gestão de Continuidade de Negócios (SGCN) unificado, garantindo a integração de seus objetivos, processos, métodos e procedimentos para sua efetiva implementação e operacionalização.

Art. 5° O SGCN deve estabelecer um modelo de processo, por meio do PCO e do PRD, que integram o ciclo de gestão de continuidade de negócios, definindo papéis, responsabilidades, atividades e métodos padronizados para toda a CGE-RJ.

Art. 6° O SGCN deve ser orientado pelos objetivos e metas estratégicas da CGE-RJ considerando os requisitos legais e regulatórios aplicáveis.

Art. 7° O SGCN deve garantir que haja comprometimento e apoio institucional para sua efetiva operacionalização.

Art. 8° O SGCN deve manter e dar publicidade adequada à Política de Gestão de Continuidade de Negócios às partes interessadas internas e externas, quando aplicável.

Art. 9º O SGCN deve ser revisado periodicamente e aprimorado continuamente para garantir sua relevância, eficácia e alinhamento com as necessidades da CGE-RJ.

Art. 10. A continuidade de negócios na CGE-RJ deve ser orientada aos riscos de disrupção ou indisponibilidade das funções críticas ao negócio.

Art. 11. O CGTI deve conduzir Análises de Impacto nos Negócios (BIA), como complemento as análises de riscos feitas pelas unidades administrativas para identificar todos os aspectos críticos das funções de negócios, recursos e infraestrutura, além de avaliar os possíveis impactos.

Art. 12. A Análise de Impacto nos Negócios deve ser revisada e atualizada pelas unidades administrativas em no mínimo, a cada 12 (doze) meses ou de acordo com as mudanças relevantes nas operações de negócio e/ou de suas dependências.

Art. 13. O SGCN deve elaborar e manter um programa de exercícios e testes de planos de continuidade de negócios, com objetivo de treinar os envolvidos, atualizar informações e mudanças relevantes nos planos, além de melhorar os procedimentos estabelecidos.

Art. 14. As estratégias do SGCN devem ser integradas com as políticas e procedimentos de Segurança da Informação, visando assegurar a proteção, disponibilidade, integridade e confidencialidade dos sistemas e dados críticos da CGE-RJ.

6. PAPÉIS E RESPONSABILIDADES

Art. 15. Cabe à Alta Gestão da CGE-RJ:

I. aprovar a Política de Gestão de Continuidade de Negócios e o programa de revisão dos planos;

II. supervisionar o processo de gestão de continuidade de negócios, por meio de relatórios regulares da Assessoria de Tecnologia da Informação (ASSTINF);

III. garantir a disponibilidade de recursos necessários para a consecução dos objetivos da continuidade de negócios;

IV. assumir a responsabilidade pela gestão de continuidade de negócios.

Art. 16. Cabe à Assessoria de Tecnologia da Informação (ASSTINF):

I. coordenar, manter, monitorar e aprimorar o sistema de gestão de continuidade de negócios (SGCN);

II. propor, desenvolver e gerenciar os objetivos e metas de continuidade de negócios, em alinhamento com a estratégia da Alta Gestão;

III. propor necessidades de recursos à Alta Gestão da CGE-RJ para consecução dos objetivos de continuidade de negócios;

IV. promover a cultura de continuidade de negócios junto às demais unidades administrativas da CGE-RJ;

V. definir indicadores e conduzir a avaliação da eficácia do SGCN;

VI. conduzir programas de testes e exercícios do SGCN;

VII. gerenciar a documentação de continuidade de negócios;

VIII. assegurar a implementação de melhorias ou correções de forma tempestiva.

Art. 17. Cabe ao Comitê Integrado de Governança de Tecnologia e Segurança da Informação da Controladoria Geral do Estado do Rio de Janeiro – CGTI:

I. acompanhar, em nível estratégico, os resultados consolidados do SGCN, com base em relatórios, indicadores e resultados de testes;

II. deliberar sobre temas propostos pela Alta Gestão da CGE-RJ no direcionamento estratégico da Gestão de Continuidade de Negócios, quando demandado;

III. instituir grupos de trabalho, quando necessário, para tratar de temas específicos relacionados à continuidade de negócios;

IV. propor recomendações quanto à priorização de ações e necessidades de recursos relacionadas à continuidade de negócios.

Art. 18. Cabe às unidades administrativas responsáveis pelos processos:

I. elaborar, revisar, manter e aprimorar continuamente os planos de continuidade relacionados aos seus processos, incluindo a implementação de melhorias identificadas;

II. elaborar a análise de riscos para identificar os aspectos críticos das funções de negócios, recursos e infraestrutura, além de avaliar os possíveis impactos;

III. comunicar mudanças que afetem os processos que possuam planos de continuidade de negócios;

IV. cumprir as ações previstas nos planos de continuidade durante sua ativação;

V. participar de treinamentos e exercícios de continuidade de negócios.

7. Disposições Finais

Art. 19. Esta Política está alinhada com as demais políticas e normas da CGE-RJ.

Art. 20. A CGE-RJ, por meio de seus respectivos gestores e equipes, é responsável por assegurar a implementação e o cumprimento dos princípios e diretrizes estabelecidos nesta Política.

Art. 21. Esta Política deve ser revisada periodicamente, em no mínimo 12 (doze) meses, ou sempre que mudanças significativas na organização, nos riscos, nos processos críticos ou no ambiente regulatório assim exigirem, visando sua atualização e adequação contínua.

Art. 22. O descumprimento das diretrizes estabelecidas nesta Política sujeitará o agente envolvido às sanções administrativas cabíveis, conforme previsto na legislação vigente e nas demais normas internas da CGE-RJ.

Art. 23. Esta Política entra em vigor na data de sua publicação. Os casos omissos e as dúvidas na interpretação desta Política serão discutidos pelo Comitê Integrado de Governança de Tecnologia e Segurança da Informação da Controladoria Geral do Estado do Rio de Janeiro (CGTI).

REFERÊNCIAS

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001: Segurança da informação, segurança cibernética e proteção da privacidade — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro: ABNT, 2022.

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002: Segurança da informação, segurança cibernética e proteção da privacidade — Controles de segurança da informação. Rio de Janeiro: ABNT, 2022.

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27701: Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da informação de privacidade — Requisitos e diretrizes. Rio de Janeiro: ABNT, 2019.

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 22301: Segurança e resiliência — Sistemas de gestão de continuidade de negócios — Requisitos. Rio de Janeiro: ABNT, 2020.

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT ISO/TS 22317: Temas relativos à segurança — Sistemas de gestão da continuidade dos negócios — Diretrizes para análise de impacto nos negócios (BIA). Rio de Janeiro: ABNT, 2023.

- BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 21 ago. 2026.

- RIO DE JANEIRO (Estado). Decreto nº 48.891, de 11 de janeiro de 2024. Dispõe sobre a Política de Governança em Privacidade e Proteção de Dados Pessoais no âmbito do Poder Executivo do Estado do Rio de Janeiro. Diário Oficial do Estado do Rio de Janeiro, Rio de Janeiro, 12 jan. 2024.

- RIO DE JANEIRO (Estado). Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro (PRODERJ). Portaria PRODERJ/PRE nº 968, de 2022. Apróva o Manual de Procedimentos Regulatórios de Segurança da Informação. Rio de Janeiro: PRODERJ, 2022.

CONTROLADORIA GERAL

GOV RJ