DELIBERAÇÃO

GR-016/2024

Data Início:

Data Fim:

CÓDIGO DE CLASSIFICAÇÃO ARQUIVÍSTICA: 010.01 **CLASSIFICAÇÃO DA INFORMAÇÃO:** Ostensivo

TÍTULO: **POLÍTICA CORPORATIVA DE CONTINUIDADE DE NEGÓCIOS – PCCN**

PALAVRAS – CHAVE: política corporativa de continuidade de negócios, continuidade de negócios, pccn, smc, ici, rto, rpo, disrupção, processos críticos, gcn, pcn

ANEXO:

1 – Política Corporativa de Continuidade de Negócios – PCCN

PROCESSO: 12.05 - Gerenciar Continuidade de Negócios

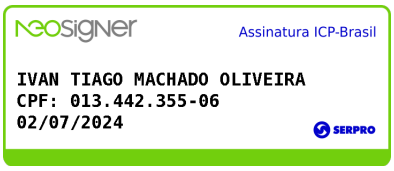
O CONSELHO DE ADMINISTRAÇÃO DO SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS – SERPRO, no uso das competências que lhe atribui o art. 19, inciso II, do Estatuto Social do SERPRO.

DELIBERA

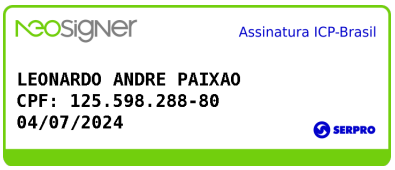
1.0 Alterar a Política Corporativa de Continuidade de Negócios (PCCN), constante do Anexo 1 desta Deliberação, com o objetivo de fornecer o direcionamento estratégico da continuidade de negócio para o Serpro.

2.0 Cancelar a Deliberação RI-010/2021, de 12 de maio de 2021.

FERNANDO FERREIRA
Presidente do Conselho de Administração

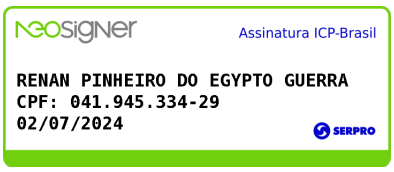


IVAN TIAGO MACHADO OLIVEIRA
Conselheiro

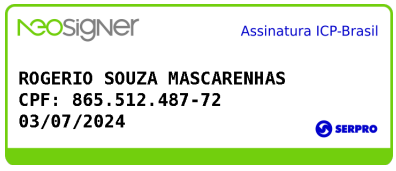


LEONARDO ANDRÉ PAIXÃO
Conselheiro Independente

MANOEL TAVARES DE MENEZES NETTO
Conselheiro



RENAN PINHEIRO DO EGYPTO GUERRA
Conselheiro Representante dos Empregados



ROGÉRIO SOUZA MASCARENHAS
Conselheiro

ÓRGÃO/REDATOR: DIOPE/SUPSI/SIGSC/SIRSC/rog

1.0 OBJETIVO

Estabelecer o direcionamento estratégico para a Continuidade de Negócios do Serpro em situações de emergência ou desastre.

2.0 ÂMBITO DE APLICAÇÃO

Todos os órgãos da empresa.

3.0 DEFINIÇÕES

Para efeito desta Política, entende-se por:

a) Continuidade de negócio: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, a fim de manter suas operações em um nível aceitável, previamente definido;

b) Desastre: evento, ação ou omissão, repentino e não planejado, que tenha permitido acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica, gerando sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;

c) Disrupção: incidente antecipado ou imprevisto que resulta em desvios negativos e não planejados na entrega esperada de produtos e serviços de acordo com os objetivos da organização.

d) Emergência: evento ou ocorrência inesperada, geralmente urgente e repentina, que requer ação imediata.

e) Infraestrutura Crítica Interna (ICI): instalações, ativos e plataformas que suportam SMC;

f) Objetivos de recuperação: conjunto de informações formado pelo tempo objetivado de recuperação (RTO) e pelo ponto objetivado de recuperação (RPO);

g) Plano de Continuidade de Negócio (PCN): documentação de procedimentos e informações desenvolvida, consolidada e mantida de forma que esteja pronta para uso caso ocorra um incidente, de modo a permitir que a organização mantenha suas atividades críticas em um nível aceitável previamente definido;

g.1) Plano de Continuidade de Negócios em Segurança da Informação: documentação dos procedimentos e das informações necessárias para que os órgãos ou entidades da administração pública federal mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo, em um nível previamente definido, em caso de incidente. Essa documentação é parte do Plano de Continuidade de Negócio (PCN), especializada em Segurança da Informação;

h) Ponto objetivado de recuperação (RPO): período máximo desejado antes de uma falha ou desastre durante o qual as alterações feitas aos dados podem ser perdidas como processo de uma recuperação;

i) Processos críticos: aqueles considerados primordiais para o atendimento das finalidades e objetivos estatutários, classificados de acordo com critérios de materialidade, relevância e criticidade;

j) Serviço de Missão Crítica (SMC): serviço cuja paralisação ou perda de dados podem gerar impactos negativos para o negócio. No caso do Serpro, os SMC pertencem a uma das categorias: serviços internos ou serviços multiclientes indicados pela Administração da empresa, ou serviços sob medida apontados pelos clientes ou pela Diretoria de Relacionamento com Clientes; e

k) Tempo objetivado de recuperação (RTO): tempo máximo permitido para recuperação de um serviço após uma disrupção.

4.0 PREMISSAS

4.1 O escopo da Gestão de Continuidade de Negócios – GCN do Serpro compreende os SMC, as ICI e os processos críticos.

4.2 A capacidade de continuidade de negócios deve estar coerente à criticidade, sensibilidade e complexidade do escopo.

4.3 A Gestão de Continuidade de Negócios do Serpro deve estar em conformidade com as estratégias empresariais, legislação, normas, melhores práticas e contratos.

4.4 A Gestão de Continuidade de Negócios do Serpro deve estabelecer uma estrutura que permita responder efetivamente nas situações de risco, emergência ou desastre e salvaguardar as pessoas, as necessidades e expectativas das partes interessadas, a reputação e a marca da organização.

4.5 Os SMC, as ICI e os processos críticos que exijam a abordagem de Continuidade de Negócios devem ter seus dados e sistemas protegidos e possuir mecanismos que garantam sua recuperação em caso de disrupção significativa.

4.6 A Segurança da Informação deve ser mantida em um nível apropriado durante uma disrupção.

5.0 DETERMINAÇÕES

5.1 A documentação de Continuidade de Negócios deve ser mantida atualizada, protegida e disponível de acordo com o seu grau de sigilo.

5.2 A Gestão de Continuidade de Negócios deve seguir as etapas do respectivo processo “Gerenciar Continuidade de Negócios”.

5.2.1 Os impactos resultantes de disrupção ou desastre, as funções principais, as prioridades de recuperação e as interdependências devem ser identificados, de forma a atender aos

objetivos de recuperação definidos.

5.2.2 Os riscos devem ser avaliados e tratados de forma a ter controles adequados, considerando a relação custo-benefício.

5.2.3 A estratégia de continuidade de negócios deve estar adequada aos impactos e aos riscos identificados.

5.2.4 Os Planos de Continuidade de Negócios – PCN devem ser testados e revisados periodicamente.

5.3 As ações de cultura em continuidade devem ser permanentemente fortalecidas, de forma a assegurar que empregados e partes externas cumpram suas obrigações e responsabilidades, relacionadas à Gestão de Continuidade de Negócios.

6.0 RESPONSÁVEIS

6.1 O Comitê Estratégico de Governança, Riscos, Controles e Segurança da Informação – COGRS é o órgão colegiado de pronúncia, atualização e proteção da PCCN.

6.2 A Superintendência de Segurança da Informação - SUPSI é responsável pela manutenção desta Política e pela gestão do processo de Continuidade de Negócios.

6.3 As Unidades são responsáveis pela avaliação da implementação da PCCN, pela coordenação do ciclo de vida dos planos de continuidade e pela prestação de contas relativa às ações de GCN no seu segmento de atuação.

6.3.1 Quando pertinente, as Unidades são responsáveis pela coordenação da criação e da manutenção dos planos de continuidade e pela prestação de contas relativa às ações de GCN, sob sua gestão, de acordo com a PCCN.

6.3.2 As Unidades de Relacionamento com Clientes são responsáveis por viabilizar a entrega da continuidade de negócios firmada em contratos.

6.3.3 A Superintendência de Gestão, Processos, Privacidade e Proteção de Dados Pessoais – SUPPP é responsável por coordenar e orientar a identificação dos critérios para definição dos processos críticos.

6.3.4 A Superintendência de Controles, Riscos e Conformidade – SUPCR é responsável por direcionar e orientar a elaboração dos planos de contingência para os processos críticos.

6.3.5 A Superintendência de Segurança da Informação – SUPSI é responsável por direcionar e orientar a elaboração dos planos de continuidade dos SMCs e ICIs.

7.0 DISPOSIÇÕES FINAIS

7.1 A PCCN deve ser revisada a cada três anos ou nas situações que representem alterações significativas nos processos ou estrutura do Serpro.

7.2 O Programa de Gestão de Continuidade de Negócios – PGCN contempla o modelo de

governança e de gestão da continuidade de negócios e tem como objetivo atender as orientações desta Política.

7.3 A Gestão de Continuidade de Negócios no Serpro tem como referência as orientações dos seguintes documentos:

a) ABNT NBR ISO 22301:2020 (Segurança e resiliência — Sistema de gestão de continuidade de negócios — Requisitos);

b) ABNT NBR ISO 22313:2020 (Segurança e resiliência — Sistemas de gestão de continuidade de negócios — Orientações para o uso da ABNT NBR ISO 22301);

c) ABNT NBR ISO/IEC 27002:2022 (Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação);

d) INSTRUÇÃO NORMATIVA GSI/PR Nº 3, DE 28 DE MAIO DE 2021;

e) PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021; e

f) ISO 22300:2018 (Security and resilience — Vocabulary).