Governo do Estado de São Paulo
Fundação Centro de Atendimento Socioeducativo ao Adolescente
ATI - Assessoria de Tecnologia da Informação

INSTRUÇÃO

Nº do Processo: 161.00076207/2025-23

Interessado: FUNDAÇÃO CASA, ATI - Assessoria de Tecnologia da Informação

Assunto: Política de Continuidade Operacional de TI

Responsável	Assessoria de Tecnologia da Informação - ATI
Aprovado por:	Gabinete da Presidência.
Políticas Relacionadas	Política de Governança de TI, Política de Segurança da Informação, Política de Gestão de Incidentes e Problemas, Política de Proteção de Dados e Privacidade, Política de Gestão de Capacidade e Desempenho
Localização de armazenamento	Processo SEI 161.000762/2025-23
Data da Aprovação	Data da Assinatura
Data de revisão	
Versão	1.0

TERMOS E CONDIÇÕES

BIA – Business Impact Analysis (Análise de Impacto nos Negócios): Processo que avalia os impactos potenciais de interrupções nas operações, identificando funções críticas e determinando requisitos para sua recuperação.

Crises ou Desastres: Eventos graves que afetam significativamente as operações da organização, podendo comprometer serviços essenciais, segurança de dados ou infraestrutura tecnológica.

Failover: Mecanismo de redundância que permite a transferência automática de uma operação para um sistema de backup em caso de falha do sistema principal.

Falhas: Problemas técnicos ou operacionais que afetam o funcionamento normal de um sistema, mas que podem ser resolvidos sem grandes impactos.

Incidentes: Eventos não planejados que afetam a integridade, disponibilidade ou segurança dos sistemas, podendo exigir resposta imediata para evitar impactos maiores.

MTTR – Mean Time to Recovery (Tempo Médio de Recuperação) : Métrica que indica o tempo médio necessário para restaurar um sistema após uma falha ou incidente.

PAC – Plano de Administração de Crises: Conjunto de estratégias e diretrizes para gerenciar e minimizar impactos de crises organizacionais, garantindo uma resposta eficaz.

PCO – Plano de Continuidade Operacional: Estratégia para manter ou restabelecer operações críticas em caso de falhas, incidentes ou desastres, minimizando interrupções.

PRD – Plano de Recuperação de Desastres: Plano detalhado para restaurar infraestrutura de TI e serviços após um desastre, garantindo a retomada das operações dentro dos prazos estabelecidos.

RPO – Recovery Point Objective (Objetivo de Ponto de Recuperação): Define a quantidade máxima de dados que pode ser perdida em um incidente sem comprometer a operação, determinando a frequência dos backups.

RTO – Recovery Time Objective (Objetivo de Tempo de Recuperação) : Tempo máximo aceitável para restaurar operações após uma falha ou desastre, garantindo a retomada dos serviços essenciais.

REFERÊNCIAS LEGAIS E BOAS PRÁTICAS

Referência	Descrição e Uso na Política
ISO/IEC 27001	Norma internacional de gestão da segurança da informação, garantindo a proteção dos dados e a resiliência dos serviços críticos. Usada para alinhamento das diretrizes de segurança no Plano de Continuidade Operacional (PCO).
ISO/IEC 22301	Norma internacional para sistemas de gestão da continuidade de negócios (SGCN), fornecendo diretrizes para planejamento e implementação da continuidade operacional. Base para estruturação do PCO e do Plano de Administração de Crises (PAC).
ITIL (Information Technology Infrastructure Library)	Conjunto de boas práticas para gerenciamento de serviços de TI, incluindo gestão de incidentes, problemas e continuidade de serviços. Aplicada na definição de processos de recuperação e resposta a crises.
COBIT (Control Objectives for Information and Related Technologies)	Framework para governança e gestão de TI, garantindo alinhamento entre continuidade operacional e objetivos estratégicos da organização. Utilizado na estrutura de governança e responsabilidades.

NIST SP 800-34	Guia do Instituto Nacional de Padrões e Tecnologia dos EUA para planejamento de recuperação de TI após desastres. Referência para o Plano de Recuperação de Desastres (PRD).
ISO/IEC 27035	Norma que trata da gestão de incidentes de segurança da informação, auxiliando na definição de critérios de ativação do PAC.
LGPD (Lei Geral de Proteção de Dados - Lei nº 13.709/2018)	Legislação brasileira que regulamenta o tratamento de dados pessoais. Impacta os planos de continuidade ao exigir proteção e recuperação adequada de informações sensíveis.
COSO ERM (Enterprise Risk Management - Integrated Framework)	Framework de gestão de riscos corporativos que auxilia na integração entre gestão de riscos e continuidade operacional. Aplicado na definição da estratégia de mitigação de riscos de TI.
PMBOK (Project Management Body of Knowledge)	Guia de boas práticas em gerenciamento de projetos. Utilizado na implementação e revisão dos planos de continuidade e recuperação.
BCP (Business Continuity Planning)	Conjunto de práticas para garantir a continuidade dos negócios em situações adversas. Base para estruturação dos planos de continuidade e recuperação.

CAPÍTULO I – DISPOSIÇÕES GERAIS

Seção I – Objetivo

Artigo 1º Esta Política tem por objetivo estabelecer diretrizes e procedimentos para garantir a continuidade dos serviços de Tecnologia da Informação (TI) diante de eventos adversos que possam comprometer sua disponibilidade, integridade e confiabilidade.

Artigo 2º A Política de Continuidade Operacional de TI visa reduzir impactos em caso de falhas, incidentes, crises ou desastres, assegurando a recuperação eficiente dos serviços essenciais e a manutenção das atividades institucionais.

Artigo 3º Esta Política está alinhada às melhores práticas de gestão de continuidade, incluindo ITIL, COBIT e normas ISO relacionadas, promovendo uma abordagem estruturada para prevenção e resposta a incidentes.

Seção II – Abrangência

Artigo 4º Esta Política se aplica a todos os serviços, sistemas, infraestrutura, processos e ativos

de TI da instituição, bem como a colaboradores, prestadores de serviço e demais partes envolvidas na gestão e operação dos serviços de TI.

Artigo 5º Estão abrangidos por esta Política os seguintes elementos:

I. Sistemas de informação críticos para a execução das atividades institucionais;

II. Infraestrutura de TI, incluindo servidores, redes, armazenamento de dados e comunicação;

III. Processos e procedimentos relacionados à continuidade e recuperação de serviços;

IV. Equipes responsáveis pela execução e monitoramento dos planos de continuidade;

V. Fornecedores e prestadores de serviço que atuam na operação e suporte dos serviços de TI.

Seção III – Princípios e Diretrizes

Artigo 6º A continuidade operacional de TI será pautada pelos seguintes princípios:

I. **Disponibilidade**: Garantia de acesso contínuo e confiável aos sistemas e serviços de TI essenciais;

II. **Integridade**: Manutenção da precisão e confiabilidade das informações armazenadas e processadas pelos sistemas;

III. **Resiliência**: Capacidade de resposta, adaptação e recuperação diante de incidentes e crises;

IV. **Segurança**: Proteção contra ameaças internas e externas que possam comprometer a continuidade operacional;

V. **Melhoria Contínua**: Atualização periódica dos planos e processos, com base em testes, auditorias e lições aprendidas.

Artigo 7º Para garantir a efetividade desta Política, serão adotadas as seguintes diretrizes:

I. Desenvolvimento e implementação do Plano de Continuidade Operacional de TI (PCO), Plano de Administração de Crises (PAC) e Plano de Recuperação de Desastres (PRD);

II. Realização de testes e simulações periódicas para validação dos planos e procedimentos;

III. Definição de papéis e responsabilidades claras para a gestão da continuidade de TI;

IV. Monitoramento contínuo dos riscos e adoção de medidas preventivas para mitigação de impactos;

V. Integração com as demais políticas institucionais, garantindo alinhamento com a gestão de riscos, segurança da informação e governança de TI.

CAPÍTULO II – GOVERNANÇA E GESTÃO DA CONTINUIDADE OPERACIONAL

Seção I – Estrutura de Governança e Responsabilidades

Artigo 8º – A governança da continuidade operacional de TI será acompanhada pela Assessoria de Tecnologia da Informação – ATI em apoio ao Gabinete da Presidência.

Artigo 9º – Dos Papéis e Responsabilidades:

I. **Gabinete da Presidência**: Responsável pela definição das diretrizes, aprovação dos planos de

continuidade e aprovação da política.

II. **Gestão de TI**: Responsável pela revisão periódica das políticas e planos, por implementar e monitorar os planos de continuidade e recuperação.

III. **Gerência de Infraestrutura e Segurança da Informação, Gerência de Suporte ao Usuário e Núcleo de Apoio Tecnológico**: Responsáveis por avaliar ameaças e vulnerabilidades, garantindo a adequação às normativas.

IV. **Usuários e Demais Setores**: Responsáveis por aderir às diretrizes estabelecidas e participar dos treinamentos e simulações.

Seção II – Integração com a Gestão de Riscos e Segurança da Informação

Artigo 10 – A continuidade operacional deverá estar alinhada com a gestão de riscos corporativos, considerando:

I. A análise de impacto nos negócios (BIA – Business Impact Analysis);

II. A definição de limiares de risco aceitáveis para a operação de TI;

III. A implantação de medidas preventivas para mitigar riscos identificados.

Artigo 11 – As diretrizes de continuidade operacional devem estar em conformidade com a **Política de Segurança da Informação**, abrangendo:

I. O cumprimento das normas de segurança, como ISO 27001;

II. A proteção de dados sensíveis e confidenciais em cenários de contingência;

III. A definição de protocolos de comunicação segura durante crises e recuperação de desastres.

Seção III – Estratégia de Continuidade Operacional

Artigo 12 – A estratégia de continuidade operacional deverá ser baseada na classificação dos serviços críticos, na definição de planos de resposta e na recuperação eficiente dos serviços de TI.

Artigo 13 – Os planos de continuidade deverão contemplar:

I. A identificação de recursos essenciais para a manutenção dos serviços;

II. O estabelecimento de processos de redundância e tolerância a falhas;

III. A definição de indicadores de desempenho para avaliar a eficácia da continuidade operacional;

IV. A realização periódica de testes e simulações para validação dos planos.

Artigo 14 – A estratégia de continuidade deverá ser revisada periodicamente, garantindo a adequação às necessidades da Fundação CASA-SP e evoluções tecnológicas.

CAPÍTULO III – PLANO DE CONTINUIDADE OPERACIONAL DE TI (PCO)

Seção I – Definição e Objetivos do PCO

Artigo 15 – O Plano de Continuidade Operacional de TI (PCO) é o conjunto de estratégias, procedimentos e recursos definidos para garantir a manutenção ou recuperação dos serviços críticos de TI em caso de incidentes que comprometam a operação da organização.

Artigo 16 – O PCO tem como objetivos principais:

I. Garantir a continuidade dos serviços essenciais de TI, minimizando impactos operacionais;

II. Estabelecer procedimentos padronizados para resposta e recuperação em situações de crise;

III. Definir responsabilidades e fluxos de ação para situações de contingência;

IV. Preservar a integridade, disponibilidade e confidencialidade dos dados e sistemas críticos.

Seção II – Identificação de Serviços Críticos

Artigo 17 – Os serviços de TI serão classificados de acordo com sua criticidade, levando em consideração:

I. Impacto no funcionamento da organização;

II. Dependência de outras áreas e serviços;

III. Tempo máximo tolerável de indisponibilidade (RTO – Recovery Time Objective);

IV. Perdas operacionais e financeiras associadas à interrupção do serviço.

Artigo 18 – A identificação dos serviços críticos será realizada periodicamente, por meio da análise de impacto nos negócios (BIA – Business Impact Analysis), envolvendo a participação das áreas estratégicas da Fundação CASA-SP.

Seção III – Critérios de Priorização da Recuperação de Serviços

Artigo 19 – Os serviços de TI serão priorizados de acordo com:

I. O impacto da interrupção na continuidade dos processos institucionais;

II. A existência de alternativas ou redundâncias tecnológicas disponíveis;

III. A complexidade do processo de recuperação e os recursos necessários;

IV. A criticidade da informação e dos dados envolvidos.

Artigo 20 – Os prazos de recuperação serão estabelecidos com base nos seguintes parâmetros:

I. **RTO (Recovery Time Objective)**: tempo máximo aceitável para a recuperação do serviço;

II. **RPO (Recovery Point Objective)**: ponto máximo de perda de dados aceitável em caso de falha;

III. **MTTR (Mean Time to Recovery)**: tempo médio necessário para restaurar a operação.

Seção IV – Procedimentos de Manutenção e Atualização do PCO

Artigo 21 – O PCO deverá ser revisado periodicamente para garantir sua eficácia, considerando:

I. Mudanças na estrutura organizacional e tecnológica;

II. Resultados obtidos em testes e simulações;

III. Aprendizados adquiridos em incidentes reais.

Artigo 22 – Para garantir a eficácia do PCO, deverão ser conduzidos testes periódicos, incluindo:

I. Simulações de cenários de falha e resposta emergencial;

II. Testes de failover e redundância de sistemas críticos;

III. Treinamentos para equipes envolvidas na execução do plano.

Artigo 23 – A manutenção do PCO será responsabilidade da Assessoria de Tecnologia da Informação - ATI, que deverá assegurar a atualização contínua do plano com base nas melhores práticas, novos riscos identificados e evolução das necessidades organizacionais.

CAPÍTULO IV – PLANO DE ADMINISTRAÇÃO DE CRISES (PAC)

Seção I – Definição e Objetivos do PAC

Artigo 24 – O Plano de Administração de Crises (PAC) estabelece diretrizes, procedimentos e responsabilidades para a gestão de crises em Tecnologia da Informação (TI), garantindo uma resposta eficiente a incidentes que possam comprometer a continuidade dos serviços essenciais.

Artigo 25 – O PAC tem os seguintes objetivos:

I. **Assegurar a resposta coordenada a crises que impactem a infraestrutura e os serviços de TI**;

II. **Minimizar os danos operacionais, financeiros e reputacionais da organização** ;

III. **Garantir a retomada dos serviços de TI de forma estruturada e eficiente** ;

IV. **Estabelecer um fluxo claro de comunicação e tomada de decisão em momentos críticos** ;

V. **Promover a preparação e capacitação da equipe para resposta a crises** .

Seção II – Critérios de Ativação do PAC

Artigo 26 – Para efeitos desta política, considera-se crise qualquer evento ou incidente de TI que:

I. **Interrompa total ou parcialmente serviços críticos da organização**;

II. **Exceda os tempos de recuperação definidos no Plano de Continuidade Operacional (PCO)**;

III. **Afete diretamente a segurança da informação ou a integridade dos dados da organização**;

IV. **Tenha impacto significativo nas operações da organização ou nos clientes/usuários dos serviços de TI**.

Artigo 27 – As crises de TI serão classificadas em três níveis:

I. **Crise de Nível 1 (Baixo Impacto)**: afeta um número reduzido de usuários ou serviços, podendo ser resolvida rapidamente sem impacto significativo.

II. **Crise de Nível 2 (Impacto Moderado)**: compromete serviços essenciais, exigindo a mobilização de equipes especializadas.

III. **Crise de Nível 3 (Alto Impacto/Catástrofe)**: paralisa serviços críticos e exige ativação total do PAC e comunicação com a alta administração.

Artigo 28 – A ativação do PAC será realizada por meio dos seguintes passos:

I. **Identificação e registro do incidente/crise** por qualquer colaborador ou sistema de monitoramento;

II. **Avaliação inicial do impacto e gravidade pela equipe de TI e segurança da informação** ;

III. **Encaminhamento à Assessoria de Tecnologia da Informação** para análise e tomada de decisão, quando necessário em conjunto com o Gabinete da Presidência;

IV. **Definição das ações de resposta e mitigação conforme os procedimentos estabelecidos no PAC**;

V. **Monitoramento contínuo e ajustes na resposta, conforme necessário**.

Seção III – Procedimentos para Gestão de Crises

Artigo 29 – A resposta a uma crise de TI será conduzida em quatro fases:

I. **Detecção e Avaliação**: identificação do incidente, análise do impacto e classificação da crise.

II. **Resposta Imediata**: contenção do problema, mitigação de impactos e comunicação inicial às partes envolvidas.

III. **Recuperação e Restauração**: aplicação dos procedimentos técnicos necessários para restabelecimento dos serviços.

IV. **Análise Pós-Crise**: avaliação dos eventos ocorridos, documentação das lições aprendidas e proposição de melhorias nos planos de continuidade e administração de crises.

Artigo 30 – Para uma resposta eficaz, serão utilizados os seguintes recursos:

I. **Monitoramento contínuo dos sistemas e serviços críticos** para detecção antecipada de falhas;

II. **Automação de respostas a incidentes sempre que possível**, visando agilizar a contenção de danos;

III. **Simulações e treinamentos periódicos** para preparar as equipes para crises reais;

IV. **Planos de contingência alternativos** para assegurar a continuidade dos serviços essenciais.

Seção IV – Comunicação e Tomada de Decisão em Situações Críticas

Artigo 31 – A comunicação durante crises deverá seguir um fluxo estruturado, garantindo clareza e eficiência:

I. **Definição de uma equipe responsável pela comunicação interna e externa** sobre o incidente;

II. **Manutenção de canais seguros de comunicação**, evitando disseminação de informações imprecisas;

III. **Atualizações regulares para stakeholders internos e externos**, conforme necessário;

IV. **Uso de um sistema de registro de incidentes** para documentar todas as ações e decisões tomadas.

Artigo 32 – A ATI em conjunto com o Gabinete da Presidência terá as seguintes responsabilidades:

I. **Tomada de decisão sobre a ativação e encerramento do PAC**;

II. **Definição e priorização das ações de resposta e mitigação**;

III. **Avaliação dos impactos da crise e recomendação de medidas corretivas**;

IV. **Revisão dos planos de continuidade e gestão de crises com base nas lições aprendidas**.

Artigo 33 – Após a resolução de uma crise, deverá ser realizada uma análise retrospectiva, contemplando:

I. **Documentação detalhada dos eventos e ações tomadas**;

II. **Identificação de falhas no processo de resposta e recuperação**;

III. **Revisão e atualização dos planos de continuidade e administração de crises**;

IV. **Treinamento das equipes com base nas lições aprendidas**.

CAPÍTULO V – PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

Seção I – Definição e Objetivos do PRD

Artigo 34 – O Plano de Recuperação de Desastres (PRD) estabelece diretrizes, procedimentos e responsabilidades para restaurar a infraestrutura e os serviços de Tecnologia da Informação (TI) após um desastre, garantindo a continuidade operacional e minimizando impactos à organização.

Artigo 35 – O PRD tem os seguintes objetivos:

I. **Assegurar a rápida recuperação dos sistemas e serviços de TI em caso de desastres**;

II. **Minimizar as interrupções operacionais e os impactos financeiros e reputacionais da organização**;

III. **Definir estratégias e prioridades para a restauração de serviços críticos**;

IV. **Estabelecer um plano estruturado de testes e simulações para validar a eficácia do PRD**;

V. **Garantir que os procedimentos de recuperação sejam atualizados conforme as melhores práticas e necessidades organizacionais**.

Seção II – Estratégias de Recuperação Tecnológica

Artigo 36 – Para efeitos deste plano, desastres em TI são classificados em:

I. **Desastres Naturais**: enchentes, incêndios, terremotos ou qualquer evento ambiental que comprometa a infraestrutura de TI;

II. **Falhas Técnicas Críticas**: panes em servidores, redes, bancos de dados, data centers ou sistemas essenciais;

III. **Ataques Cibernéticos**: incidentes de segurança como ransomware, vazamento de dados ou acesso não autorizado;

IV. **Erro Humano ou Interno**: falhas operacionais, configurações indevidas ou exclusão acidental de dados críticos.

Artigo 37 – Para cada tipo de desastre, serão adotadas estratégias específicas, incluindo:

I. **Redundância de Infraestrutura**: replicação de servidores e serviços em locais distintos;

II. **Backup e Restauração**: políticas rigorosas de backup com cópias armazenadas em locais seguros e procedimentos documentados de recuperação;

III. **Ambientes de Recuperação**: definição de sites de contingência, conforme criticidade dos serviços;

IV. **Automação da Recuperação**: utilização de scripts e ferramentas de automação para restaurar serviços rapidamente;

V. **Planos de Continuidade para Fornecedores**: garantia de que parceiros estratégicos também possuam planos robustos de recuperação.

Seção III – Testes e Simulações do PRD

Artigo 38 – Os testes e simulações do PRD são fundamentais para garantir que os procedimentos de recuperação sejam eficazes e possam ser executados conforme planejado.

Artigo 39 – São tipos de testes que poderão ser realizados:

I. **Teste de Mesa (Tabletop Exercise)**: simulação teórica em que a equipe analisa e discute as ações a serem tomadas diante de um cenário de desastre hipotético;

II. **Teste Parcial**: validação da recuperação de componentes específicos do PRD sem impacto real nas operações;

III. **Teste Completo (Full Recovery Test)**: restauração completa de um ambiente crítico para validar a efetividade do PRD;

IV. **Teste de Backup e Restauração**: verificação periódica da integridade dos backups e tempo necessário para restauração.

Seção IV – Procedimentos de Retorno à Operação Normal

Artigo 40 – O retorno das operações normais será autorizado quando:

I. **Os sistemas críticos forem restaurados e validados** conforme os procedimentos estabelecidos;

II. **Os impactos operacionais e de segurança forem mitigados** de maneira satisfatória;

III. **Os usuários forem devidamente informados** sobre a retomada dos serviços;

IV. **Os registros e logs do incidente forem documentados** para análise pós-desastre.

Artigo 41 – Após a restauração dos serviços, será implementado um plano de monitoramento para:

I. **Identificar possíveis falhas remanescentes** ou novos riscos decorrentes do desastre;

II. **Garantir que os sistemas estejam operando conforme esperado** ;

III. **Realizar ajustes nos procedimentos do PRD** com base nas lições aprendidas.

Artigo 42 – O PRD será revisado e atualizado periodicamente para:

I. **Adequação às novas tecnologias e mudanças na infraestrutura de TI** ;

II. **Correção de falhas identificadas nos testes e simulações** ;

III. **Melhoria contínua dos procedimentos e estratégias de recuperação** .

CAPÍTULO VIII – DISPOSIÇÕES FINAIS

Artigo 43 – Esta política será revisada periodicamente, conforme a necessidade e evolução das melhores práticas de governança de TI, segurança da informação e mudanças na legislação aplicável.

Artigo 44 – Alterações na Política deverão ser submetidas à aprovação do Gabinete da Presidência.

São Paulo, na data da assinatura digital.

Raelen Bego Luiz
Chefe de Gabinete

Leandro Timossi de Almeida
Assessor da Presidência

Documento assinado eletronicamente por **Leandro Timossi de Almeida**, **Assessor da Presidência II**, em 24/03/2025, às 12:51, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Raelen Bego Luiz**, **Chefe de Gabinete**, em 24/03/2025, às 17:21, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

A autenticidade deste documento pode ser conferida no site https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0060856285** e o código CRC **6700D001**.