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

INSTRUÇÃO

Nº do Processo: 161.00063490/2025-23

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

Assunto: Política de Gestão de Incidentes e Problemas

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 Continuidade Operacional de TI
Localização de armazenamento	Processo SEI 161.00063490/2025-23
Data da Aprovação	Data da Assinatura
Data de revisão	
Versão	1.0

Referências Legais e Boas Práticas

Referência	Descrição e Aplicação
ITIL (Information Technology Infrastructure Library)	Conjunto de boas práticas para a gestão de serviços de TI. A política adota conceitos de **Gestão de Incidentes** e **Gestão de Problemas**, incluindo a diferenciação entre ambos, classificação, registro, análise de causa raiz e gerenciamento de erros conhecidos.

ISO/IEC 20000	Norma internacional para gerenciamento de serviços de TI. A política alinha-se com os processos padronizados para **suporte a serviços**, garantindo eficiência e qualidade no tratamento de incidentes e problemas.
ISO/IEC 27001	Norma internacional de gestão de segurança da informação. Aplica-se à política na parte de **incidentes de segurança da informação**, integrando-se com a Política de Segurança da Informação para mitigação de riscos.
Resolução CGSI nº 6/2021 (GSI/PR)	Regulamenta a gestão de incidentes de segurança cibernética no Brasil. A política adota diretrizes dessa resolução para incidentes de TI que envolvam segurança da informação e resposta a ameaças.
Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018	A política contempla a necessidade de tratamento adequado de incidentes e problemas relacionados a **dados pessoais**, alinhando-se às exigências da LGPD, especialmente no caso de **vazamentos de dados**.
NIST SP 800-61 (Computer Security Incident Handling Guide)	Diretrizes do NIST para tratamento de incidentes de segurança. A política adota recomendações para **registro, resposta e mitigação** de incidentes de TI.
COBIT (Control Objectives for Information and Related Technologies)	Framework de governança de TI. Utilizado na política para garantir que os processos de **gestão de incidentes e problemas** estejam alinhados aos objetivos estratégicos da organização.

CAPÍTULO I – DISPOSIÇÕES GERAIS

Seção I – Objetivo

Art. 1º – Esta Política estabelece diretrizes para a gestão de incidentes e problemas nos serviços e infraestrutura de TI, visando a rápida identificação, registro, análise, resolução e prevenção de incidentes e problemas, garantindo a eficiência e qualidade do suporte técnico.

Art. 2º – A gestão de incidentes tem como objetivo restaurar a operação normal dos serviços de TI o mais rápido possível**,** minimizando impactos aos usuários.

Art. 3º – A gestão de problemas visa identificar e eliminar as causas raiz de incidentes recorrentes, prevenindo a sua reincidência e melhorando continuamente os serviços de TI.

Art. 4º – As diretrizes desta política devem estar alinhadas às melhores práticas de mercado, incluindo ITIL, sem sobrepor-se a outras políticas institucionais de TI.

Seção II – Abrangência

Art. 5º – Esta política se aplica a todos os incidentes e problemas relacionados a sistemas, serviços, infraestrutura e dispositivos de Tecnologia da Informação sob gestão da Fundação CASA-SP.

Art. 6º – Esta Política não abrange procedimentos relacionados à recuperação de desastres e continuidade de serviços críticos, que devem ser tratados na Política de Continuidade Operacional de TI.

Art. 7º – Devem seguir esta política:

I. Todos os colaboradores da área de TI envolvidos na gestão de incidentes e problemas;

II. Usuários internos e externos que reportam incidentes e problemas nos sistemas e serviços de TI;

III. Fornecedores e prestadores de serviços de TI que tenham contratos ativos com a Fundação CASA-SP e sejam responsáveis por suporte, manutenção e operação de sistemas e infraestrutura.

Art. 8º – Esta política se aplica a todos os ambientes de TI da organização, incluindo:

I. Sistemas corporativos, aplicativos e serviços em nuvem;

II. Infraestrutura de redes, servidores e dispositivos computacionais;

III. Serviços de comunicação e colaboração, incluindo e-mails, telefonia e ferramentas de mensageria;

IV. Equipamentos e dispositivos utilizados para acesso aos sistemas e serviços de TI.

CAPÍTULO II – GESTÃO DE INCIDENTES

Seção I – Definição e Objetivos

Art. 9º – Um incidente é qualquer interrupção não planejada ou degradação na qualidade de um serviço de TI que afete sua operação normal e impacte os usuários ou processos de negócio da organização.

Art. 10 – O objetivo da gestão de incidentes é restaurar a operação normal dos serviços o mais rápido possível, garantindo o menor impacto possível aos usuários e à organização, conforme os seguintes princípios:

I. Minimizar interrupções e prejuízos à operação da Fundação CASA-SP;

II. Resolver incidentes de forma ágil e eficaz, seguindo critérios de priorização;

III. Garantir comunicação clara e tempestiva entre os envolvidos;

IV. Registrar e documentar incidentes para análise futura e melhoria contínua.

Seção II – Classificação de Incidentes

Art. 11 – Os incidentes serão classificados de acordo com critérios de impacto e urgência, conforme descrito a seguir:

I. **Impacto**: Grau de interferência do incidente nas operações da organização, podendo ser:

a) **Alto** – Impacto severo em serviços críticos ou um grande número de usuários afetados;

b) **Médio** – Impacto moderado, afetando alguns usuários ou serviços secundários;

c) **Baixo** – Impacto limitado a um usuário ou serviço não crítico.

II. **Urgência: Tempo aceitável para resolução do incidente, podendo ser:**

a) **Alta** – Requer atenção imediata para evitar impacto significativo;

b) **Média** – Pode ser resolvido dentro do tempo normal de atendimento;

c) **Baixa** – Pode ser tratado em prazos estendidos sem grande impacto.

Art. 12 – A combinação dos critérios de impacto e urgência definirá a prioridade do atendimento, conforme matriz de priorização estabelecida pela equipe de TI.

Seção III – Registro e Acompanhamento de Incidentes

Art. 13 – Todos os incidentes devem ser registrados em um sistema de gestão de chamados, contendo no mínimo as seguintes informações:

I. Data e hora do registro do incidente;

II. Nome e contato do usuário que reportou o incidente;

III. Descrição detalhada do problema e seus sintomas;

IV. Categoria e impacto do incidente;

V. Técnico responsável e status do atendimento;

VI. Histórico das ações realizadas para resolução.

Art. 14 – Os incidentes serão acompanhados por meio do sistema de chamados, com atualizações periódicas sobre seu status até a resolução.

Art. 15 – Caso um incidente não seja resolvido dentro do prazo estabelecido para sua prioridade, deverá ser escalonado para níveis superiores de suporte.

Seção IV – Resolução e Encerramento de Incidentes

Art. 16 – A resolução do incidente deve seguir as melhores práticas técnicas e, sempre que possível, utilizar soluções documentadas na base de conhecimento da organização.

Art. 17 – Um incidente será considerado resolvido quando:

I. O serviço impactado for restaurado e estiver operando normalmente;

II. O usuário afetado confirmar que o problema foi solucionado (quando aplicável);

III. A equipe de suporte validar a solução e documentar as ações tomadas.

Art. 18 – Após a resolução, o incidente será encerrado no sistema de chamados com um resumo das ações realizadas e, quando aplicável, com recomendações para evitar recorrências.

Art. 19 – Incidentes recorrentes ou de alta criticidade devem ser analisados para identificação de sua causa raiz e possíveis ações preventivas, conforme os procedimentos de gestão de problemas.

CAPÍTULO III – GESTÃO DE PROBLEMAS

Seção I – Definição e Objetivos

Art. 20 – Um problema é a causa raiz de um ou mais incidentes, podendo ser identificado proativamente ou como resultado da recorrência de incidentes similares.

Art. 21 – O objetivo da gestão de problemas é minimizar o impacto dos incidentes e evitar sua recorrência, por meio da identificação, análise e resolução das causas subjacentes, conforme os seguintes princípios:

I. Reduzir a frequência e o impacto dos incidentes, melhorando a estabilidade dos serviços de TI;

II. Identificar e eliminar as causas raiz dos problemas de forma estruturada;

III. Criar e manter uma base de erros conhecidos para acelerar a resolução de incidentes futuros;

IV. Implementar ações preventivas para aumentar a confiabilidade dos serviços.

Seção II – Detecção e Registro de Problemas

Art. 22 – Os problemas podem ser detectados por meio das seguintes fontes:

I. Análise de incidentes recorrentes que indicam uma possível causa raiz comum;

II. Monitoramento proativo da infraestrutura e dos serviços de TI;

III. Relatórios e reclamações dos usuários que evidenciem falhas persistentes;

IV. Testes e avaliações realizados pela equipe de TI;

V. Feedbacks de fornecedores e prestadores de serviço.

Art. 23 – Todos os problemas identificados devem ser registrados no sistema de gestão de chamados, contendo no mínimo as seguintes informações:

I. Data e hora do registro;

II. Descrição detalhada do problema e os incidentes associados;

III. Impacto estimado sobre os serviços e usuários;

IV. Responsável pela investigação e status do problema.

Seção III – Classificação e Priorização de Problemas

Art. 24 – Os problemas serão classificados de acordo com os seguintes critérios:

I. **Impacto**: Grau de comprometimento dos serviços de TI, podendo ser:

a) **Alto** – Problema crítico que afeta serviços essenciais ou um grande número de usuários;

b) **Médio** – Impacto moderado, afetando serviços secundários ou grupos específicos de usuários;

c) **Baixo** – Impacto reduzido, afetando poucos usuários ou serviços não críticos.

II. **Urgência**: Tempo aceitável para mitigação ou resolução do problema, podendo ser:

a) **Alta** – Exige atenção imediata para evitar impactos maiores;

b) **Média** – Pode ser tratado dentro do tempo normal de análise e resolução;

c) **Baixa** – Pode ser tratado em prazos estendidos sem afetar criticamente a organização.

Art. 25 – A combinação dos critérios de impacto e urgência definirá a prioridade do tratamento do problema, conforme matriz de priorização da equipe de TI (Anexo I).

Seção IV – Análise de Causa Raiz e Solução

Art. 26 – A análise da causa raiz será realizada utilizando técnicas estruturadas, tais como:

I. **Análise de Pareto** – Identificação dos problemas mais frequentes e seus impactos;

II. **Diagrama de Ishikawa (Espinha de Peixe)** – Mapeamento das possíveis causas de um problema;

III. **5 Porquês** – Investigação sequencial para identificar a causa raiz;

IV. **Análise de Logs e Monitoramento** – Investigação de falhas técnicas nos sistemas e infraestrutura.

Art. 27 – Após a identificação da causa raiz, serão definidas ações corretivas para sua eliminação ou mitigação, podendo incluir:

I. Correção definitiva da falha;

II. Implementação de controles para reduzir a probabilidade de recorrência;

III. Documentação de procedimentos alternativos até a solução definitiva.

Art. 28 – Sempre que possível, as ações corretivas devem ser validadas e testadas antes da implementação para evitar impactos negativos sobre o ambiente produtivo.

Seção V – Gerenciamento de Erros Conhecidos

Art. 29 – Um erro conhecido é um problema cuja causa raiz já foi identificada, mas ainda não possui uma solução definitiva.

Art. 30 – Todos os erros conhecidos devem ser documentados na Base de Erros Conhecidos, incluindo:

I. Descrição detalhada do erro e seu impacto;

II. Serviços e usuários afetados;

III. Solução temporária (workaround), se aplicável;

IV. Status do tratamento e prazo estimado para correção definitiva.

Art. 31 – A Base de Erros Conhecidos deve ser mantida acessível às equipes de suporte para acelerar a resolução de incidentes relacionados.

Seção VI – Prevenção e Melhoria Contínua

Art. 32 – A equipe de TI deve adotar medidas preventivas para reduzir a incidência de problemas, incluindo:

I. Monitoramento contínuo da infraestrutura e dos serviços de TI;

II. Aplicação de atualizações e correções de segurança regularmente;

III. Revisão e otimização dos processos de TI para identificar possíveis vulnerabilidades;

IV. Capacitação contínua da equipe de suporte técnico e desenvolvimento.

Parágrafo único – Medidas relacionadas à prevenção de falhas de grande impacto e recuperação de serviços após falhas críticas devem ser tratadas na Política de Continuidade Operacional de TI.

Art. 33 – Relatórios periódicos sobre a gestão de problemas devem ser gerados para análise e identificação de tendências, auxiliando na tomada de decisões estratégicas para melhoria da qualidade dos serviços de TI.

Art. 34 – A eficácia da gestão de problemas será avaliada periodicamente, com base em indicadores como:

I. Redução na recorrência de incidentes relacionados ao mesmo problema;

II. Tempo médio de resolução de problemas críticos;

III. Efetividade das ações preventivas implementadas.

CAPÍTULO IV – RESPONSABILIDADES

Seção I – Responsabilidades das Equipes de TI

Art. 35 – As equipes de TI são responsáveis por garantir a gestão eficaz de incidentes e problemas, assegurando a rápida resposta e a mitigação de impactos nos serviços de tecnologia da informação.

Art. 36 – Compete à **Gerência de Suporte ao Usuário**:

I. Receber, registrar e classificar incidentes reportados pelos usuários;

II. Analisar e resolver incidentes dentro do escopo de suporte de primeiro nível;

III. Escalar incidentes complexos para as equipes responsáveis conforme necessário;

IV. Informar os usuários sobre o status do incidente e as previsões de resolução;

V. Identificar a necessidade de correções ou melhorias em softwares para evitar a recorrência de incidentes;

VI. Registrar problemas recorrentes e encaminhá-los para análise da Gerência de Infraestrutura e Segurança da Informação ou do Núcleo de Apoio Tecnológico, conforme o caso.

Art. 37 – Compete à **Gerência de Infraestrutura e Segurança da Informação**:

I. Investigar e solucionar incidentes e problemas relacionados à infraestrutura de TI, redes e segurança da informação;

II. Implementar correções e melhorias para evitar a recorrência de problemas identificados;

III. Monitorar a performance dos serviços e identificar proativamente possíveis falhas;

IV. Gerenciar a Base de Erros Conhecidos e garantir que as soluções temporárias sejam documentadas e acessíveis.

Art. 38 – Compete ao Núcleo de Apoio Tecnológico:

I. Analisar e solucionar incidentes e problemas relacionados a sistemas e aplicações desenvolvidas internamente;

II. Propor ajustes nos sistemas para mitigar impactos decorrentes de falhas detectadas;

III. Coordenar a implementação de correções definitivas em sistemas e aplicativos.

Art. 39 – Compete ao Núcleo de Inteligência Organizacional:

I. Fornecer relatórios e análises baseadas em dados para apoiar a detecção de padrões de incidentes e problemas;

II. Identificar tendências e sugerir ações preventivas para a melhoria dos serviços de TI;

III. Apoiar a criação de métricas e indicadores para monitorar a eficiência da gestão de incidentes e problemas.

Art. 40 – Todas as equipes de TI devem trabalhar em conjunto para garantir que a gestão de incidentes e problemas seja eficaz, assegurando a continuidade dos serviços e a satisfação dos usuários.

Seção II – Responsabilidades dos Usuários

Art. 41 – Os usuários dos serviços de TI devem colaborar com a equipe técnica na identificação e resolução de incidentes e problemas, adotando boas práticas de uso dos sistemas e infraestrutura de TI.

Art. 42 – São responsabilidades dos usuários:

I. Reportar incidentes à equipe de Seção de Atendimento ao Usuário assim que forem identificados, fornecendo informações detalhadas sobre o problema;

II. Seguir os procedimentos recomendados pela equipe de TI para mitigar os impactos do incidente até sua resolução;

III. Manter senhas e credenciais de acesso seguras, evitando ações que comprometam a segurança da informação;

IV. Evitar tentativas de solucionar incidentes críticos sem o apoio da equipe técnica, a fim de prevenir danos maiores aos sistemas e à infraestrutura;

V. Participar de treinamentos e orientações fornecidos pela equipe de TI sobre o uso adequado dos recursos tecnológicos;

VI. Informar prontamente qualquer tentativa de acesso não autorizado ou suspeita de comprometimento da segurança dos serviços de TI.

Art. 43 – O descumprimento das responsabilidades estabelecidas nesta seção pode resultar em sanções conforme normativas internas da Fundação CASA-SP, garantindo a correta utilização dos recursos de TI.

CAPÍTULO V – MONITORAMENTO E RELATÓRIOS

Seção I – Indicadores e Métricas

Art. 44 – O monitoramento da gestão de incidentes e problemas será realizado por meio de indicadores e métricas que permitam avaliar a eficiência dos processos e a qualidade das resoluções implementadas.

Art. 45 – Os principais indicadores que podem ser utilizados incluem, mas não se limitam a:

I. Tempo Médio de Resolução de Incidentes (MTTR - Mean Time to Resolve): mede o tempo médio necessário para resolver incidentes após o registro;

II. Tempo Médio de Resolução de Problemas (MTPR - Mean Time to Problem Resolution): mede o tempo médio necessário para solucionar problemas após sua identificação;

III. Tempo Médio para Diagnóstico (MTTD - Mean Time to Diagnose): avalia o tempo médio necessário para identificar a causa raiz de um problema;

IV. Taxa de Reincidência de Incidentes: mede a frequência com que incidentes previamente resolvidos voltam a ocorrer;

V. Número de Incidentes por Categoria: permite identificar os tipos mais frequentes de incidentes e direcionar ações de melhoria;

VI. Número de Problemas Identificados Proativamente: avalia a eficácia da equipe na detecção de problemas antes de impactarem os usuários;

VII. Índice de Incidentes Resolvidos no Primeiro Contato (FCR - First Call Resolution): mede a taxa de incidentes solucionados sem a necessidade de escalonamento;

VIII. Nível de Satisfação dos Usuários: obtido por meio de pesquisas periódicas, mede a percepção dos usuários sobre a qualidade do atendimento e resolução de incidentes.

Art. 46 – A coleta e análise das métricas devem ser realizadas periodicamente, permitindo a identificação de tendências e oportunidades de otimização dos processos de gestão de incidentes e problemas.

Art. 47 – O Núcleo de Inteligência Organizacional será responsável por consolidar os dados e fornecer análises sobre os indicadores, apoiando a tomada de decisão e a implementação de ações de melhoria.

Seção II – Relatórios Periódicos e Melhoria Contínua

Art. 48 – As equipes de TI devem elaborar relatórios periódicos contendo informações detalhadas sobre a gestão de incidentes e problemas, incluindo os seguintes elementos:

I. Quantidade total de incidentes e problemas registrados no período;

II. Tempo médio de resposta e resolução de incidentes e problemas;

III. Principais categorias de incidentes e problemas;

IV. Análise das causas raízes dos problemas recorrentes;

V. Efetividade das ações corretivas e preventivas adotadas;

VI. Recomendações para a melhoria contínua dos processos de gestão de incidentes e problemas.

Art. 49 – Os relatórios periódicos deverão ser apresentados à Assessoria de Tecnologia da Informação – ATI, permitindo a definição de estratégias para aprimoramento do processo de atendimento e resolução.

Art. 50 – A melhoria contínua da gestão de incidentes e problemas será promovida por meio das seguintes práticas:

I. Análise regular dos indicadores e identificação de oportunidades de otimização dos processos;

II. Implementação de medidas corretivas e preventivas com base nos relatórios gerados;

III. Adoção de treinamentos e capacitações para as equipes técnicas e usuários, visando reduzir incidentes e melhorar a eficiência da resolução;

IV. Revisão periódica dos procedimentos para garantir alinhamento com as melhores práticas de mercado, como ITIL e demais frameworks aplicáveis.

Art. 51 – Para assuntos relacionados à continuidade dos serviços em caso de falhas críticas ou indisponibilidades prolongadas, devem ser seguidas as diretrizes estabelecidas na Política de Continuidade Operacional de TI.

Art. 52 – A política de gestão de incidentes e problemas deve ser revisada regularmente para assegurar sua aderência às necessidades da organização e à evolução das tecnologias e melhores práticas.

CAPÍTULO VI – DISPOSIÇÕES FINAIS

Art. 53 – 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.

Art. 54 – Alterações na Política deverão ser submetidas à aprovação do Gabinete da Presidência.

ANEXO I – MATRIZ DE PRIORIZAÇÃO

Matriz de priorização com base nos critérios de Impacto e Urgência para definição da prioridade do tratamento do problema.

Impacto \ Urgência	**Alta (Atenção imediata)**	**Média (Tempo normal de resolução)**	**Baixa (Prazo estendido)**
Alto (Problema crítico)	**Crítica (Prioridade 1)**	**Alta (Prioridade 2)**	**Média (Prioridade 3)**

Médio (Impacto moderado)	**Alta (Prioridade 2)**	**Média (Prioridade 3)**	**Baixa (Prioridade 4)**
Baixo (Impacto reduzido)	**Média (Prioridade 3)**	**Baixa (Prioridade 4)**	**Muito Baixa (Prioridade 5)**

Interpretação da Matriz

Prioridade 1 (Crítica): Problemas com **alto impacto e alta urgência** devem ser tratados imediatamente.

Prioridade 2 (Alta): Problemas críticos com menor urgência ou problemas moderados que exigem ação rápida.

Prioridade 3 (Média): Problemas de impacto médio com tempo de resolução aceitável ou problemas críticos com baixa urgência.

Prioridade 4 (Baixa): Problemas de menor impacto que podem ser resolvidos dentro de prazos mais longos.

Prioridade 5 (Muito Baixa): Problemas de impacto e urgência reduzidos, que podem ser tratados sem pressa.

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 13/03/2025, às 16:28, 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 18/03/2025, às 22:30, 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 **0059126980** e o código CRC **12CD55B2**.