Governo do Estado do Rio de Janeiro
Secretaria de Estado de Fazenda
Subsecretaria de Tecnologia da Informação e Comunicação

Processo de Gerenciamento de Incidentes de Tecnologia da Informação e Comunicação (TIC)

Subsecretaria de Tecnologia da Informação e Comunicação - SUBTIC

Rio de Janeiro – 2025

v.2.0

SUMÁRIO

INTRODUÇÃO

O processo de gerenciamento de incidentes de tecnologia da informação e comunicação (TIC) tem como finalidade gerenciar o ciclo de vida de todos os incidentes, assegurando um fluxo único e padronizado a fim de restaurar a operação normal dos serviços de Tecnologia da Informação e Comunicação (TIC) no menor tempo possível, reduzir impactos nas operações finalísticas da Secretaria de Estado de Fazenda do Rio de Janeiro (SEFAZ-RJ), preservar a integridade das informações e garantir o cumprimento dos níveis de serviço acordados (SLA).

ESCOPO E ABRANGÊNCIA

Este processo aplica-se a todos os serviços de TIC prestados pela Subsecretaria de Tecnologia da Informação e Comunicação (SUBTIC), sendo obrigatório para todos os incidentes registrados no âmbito da SEFAZ-RJ, incluindo, mas não se limitando a, incidentes ocorridos em hardware, redes, links de comunicação, servidores, bancos de dados, incidentes de segurança da informação e, crucialmente, falhas em sistemas de informação e aplicações corporativas sustentadas pela SUBTIC ou por fábricas de software terceirizadas.

Ficam excluídas deste fluxo as Requisições de Serviço, que consistem em solicitações de novos recursos ou acessos e devem seguir fluxo próprio, garantindo que o gerenciamento de incidentes foque exclusivamente naquilo que é uma interrupção ou redução de qualidade de um serviço existente.

TERMOS E DEFINIÇÕES

Este glossário reúne as principais definições, conceitos e termos utilizados no contexto do Gerenciamento de Incidentes de TIC da SEFAZ-RJ, alinhados às práticas e diretrizes do ITIL 4. Seu objetivo é padronizar a terminologia empregada no manual, promovendo entendimento comum entre todas as áreas envolvidas no processo. As definições aqui apresentadas servem como referência para apoiar a comunicação clara, a governança, a tomada de decisão e a correta execução das atividades associadas à gestão dos incidentes de TIC.

- **Acordo de Nível de Serviço (SLA):** Documento que define metas de atendimento, como prazos de resposta e solução.
- **Base de Conhecimento:** Repositório central com manuais, procedimentos e soluções conhecidas.
- **Incidente:** Interrupção não planejada ou redução da qualidade de um serviço de TIC.
- **Incidente Grave:** Evento com alto impacto e urgência, exigindo resposta imediata.
- **Information Technology Service Management (ITSM):** Conjunto de ferramentas e processos para gestão de serviços de TI.

- **Information Technology Infraestructure Library (ITIL4):** Versão mais recente do framework de melhores práticas para gerenciamento de serviços de TIC

DOS INCIDENTES

Todos os incidentes devem ser registrados, controlados e tratados por meio do sistema de gerenciamento de serviços de TIC. O processo deve garantir que os usuários sejam mantidos informados de suas solicitações, podendo a Central de Atendimento solicitar mais informações ao usuário quando o chamado não dispuser de informações suficientes para o atendimento.

Os chamados devem ser categorizados e priorizados pela Central de Atendimento, devendo as informações relativas à resolução ser registradas na Base de Conhecimento.

PAPÉIS E RESPONSABILIDADES

Papel	Responsabilidades	Responsável
Usuário Solicitante	• Reportar incidentes; • Fornecer evidências.	Todo servidor da SEFAZ
Central de Atendimento	• Ser o ponto único de contato; • Registrar, categorizar, priorizar e resolver incidentes simples; • Solicitar informações complementares ao usuário; • Escalonar incidentes sem solução para níveis superiores. • Inserir as informações na base de conhecimento	Central de Atendimento
Equipe Técnica	• Realizar diagnóstico técnico aprofundado; • Interagir com fornecedores externos (operadoras, fábrica de software); • Criar ou atualizar artigos da Base de Conhecimento; • Cumprir SLA de atendimento técnico.	Servidores alocados nas respectivas Superintendências
Coordenador de atendimento	• Monitorar andamento dos chamados; • Manter usuários informados; • Registrar ações corretivas e oportunidades de melhoria; • Coordenar comunicação em incidentes.	Servidores alocados na SUPINFRA

Gerente do Incidente	• Garantir eficiência e efetividade do processo; • Manter desenho do processo e indicadores atualizados; • Promover treinamentos; • Analisar melhorias e adequações; Validar mudanças de prioridades quando necessário.	Servidores alocados na SUPINFRA

DESCRIÇÃO DAS ATIVIDADES DO PROCESSO

O diagrama a seguir representa as etapas operacionais do Gerenciamento de Incidentes.

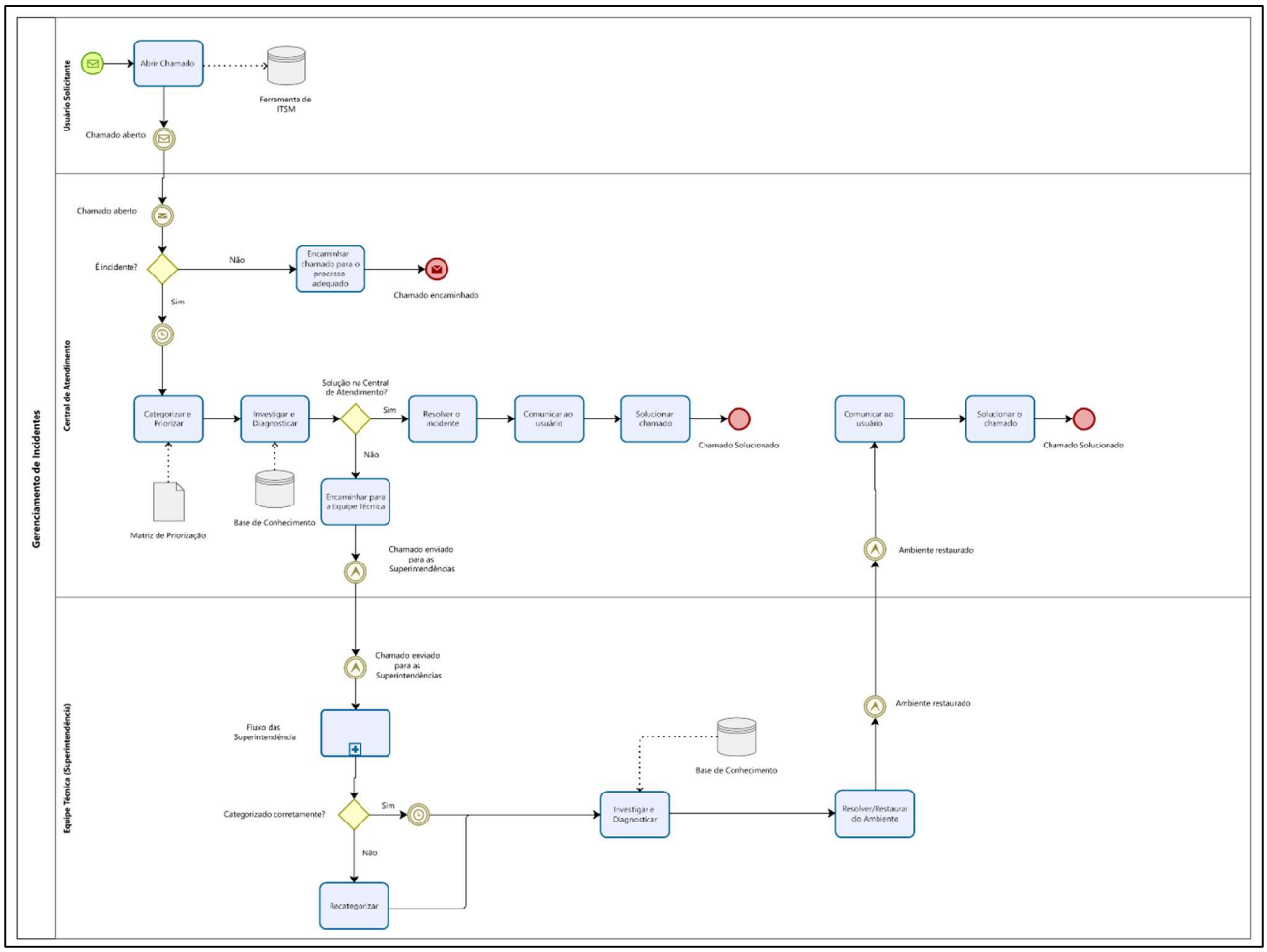

Figura 1 - Fluxo de atendimento de incidentes de TIC

De forma detalhada, o processo de Gerenciamento de Incidentes inicia-se com a abertura de um chamado pelo **Usuário Solicitante,** realizada por meio da ferramenta de Gestão de Incidentes.

Ao receber a demanda, a **Central de Atendimento** realiza a triagem inicial para verificar se a solicitação se qualifica tecnicamente como um incidente. Caso a demanda não se enquadre nesta definição, ela é encaminhada para o processo adequado.

O chamado confirmado como um incidente, a **Central de Atendimento** procede com a categorização e priorização do chamado, utilizando como referência a Matriz de Priorização. Em seguida, inicia-se a etapa de investigação e diagnóstico inicial, apoiada pela consulta à Base de Conhecimento. Se a solução for possível no primeiro nível de atendimento, o analista resolve o incidente, registra a solução do chamado, encerrando o fluxo imediatamente.

Nível dp Incidentes	Alto Impacto (Todo o ambiente da SEFAZ)	Médio Impacto (Único Setor)	Baixo Impacto (Único Usuário)
Alta Urgência	Crítico	Alta	Médio
Média Urgência	Alta	Média	Baixa

Tabela 1 - Matriz de Priorização

Caso a solução não seja viável na **Central de Atendimento,** o incidente é encaminhado para a Equipe Técnica. Ao recepcionar o chamado, a **Equipe Técnica** verifica preliminarmente se a categorização atribuída está correta. Se for identificada inconsistência, o analista realiza a recategorização necessária antes de prosseguir.

Estando a categoria correta, a equipe avança para a investigação e diagnóstico aprofundado, consultando a Base de Conhecimento e executando os procedimentos técnicos específicos, os quais podem envolver o acionamento de um Fluxo Interno da Superintendência correspondente. Após identificar a causa e definir a ação corretiva, a equipe executa a resolução do incidente e a restauração do ambiente operacional, garantindo também a atualização da Base de Conhecimento.

Após a restauração, a **Equipe Técnica** soluciona o chamado. O fluxo retorna então à responsabilidade da **Central de Atendimento**, que comunica o usuário sobre a resolução e formaliza o encerramento do chamado no sistema. Com isso, o fluxo de gerenciamento do incidente é concluído.

ACORDOS DE NÍVEL DE SERVIÇO (SLA)

Para a Central de Atendimento, que atua como ponto único de contato e suporte de primeiro nível, os indicadores de tempo de resposta (ex: tempo de espera em fila) e tempo de solução em primeiro contato (FCR) seguem rigorosamente as métricas, penalidades e estipulações definidas no contrato de prestação de serviços vigente com a empresa terceirizada.

Para as superintendências ficam estabelecidos os prazos máximos para a solução definitiva ou de contorno do incidente.

Regra de contagem: O SLA para as áreas técnicas **inicia-se a contar exclusivamente a partir do momento do escalonamento (encaminhamento)** do chamado pela Central de Atendimento para a fila da equipe técnica competente.

A definição do prazo baseia-se na Prioridade do incidente (resultado da matriz de Impacto x Urgência), conforme a tabela abaixo:

Prioridade	SLA	Descrição do Impacto
Crítico	4 horas	Interrupção completa de serviços essenciais ou críticos para a SEFAZ, afetando todos os usuários ou o cidadão. Requer ação imediata.
Alta	8 horas	Degradação severa de desempenho ou falha em funções importantes que afetam um grupo grande de usuários ou um departamento inteiro, sem solução de contorno disponível.
Média	24 horas	Falhas que afetam um grupo reduzido de usuários ou falhas parciais onde existe uma solução de contorno que permite a continuidade do trabalho, ainda que com restrições.
Baixa	36 horas	Incidentes de baixo impacto, que afetam usuários individuais, ou solicitações que não impedem a execução das atividades principais do negócio.

Tabela 2 - Matriz SLA

FLUXO INTERNO DAS SUPERINTENDÊNCIAS

O Processo de Gerenciamento de Incidentes da SUBTIC estabelece o fluxo mestre de governança, desde o registro na Central de Atendimento até o encerramento. No entanto, para garantir a resolutividade técnica, é imprescindível que cada Superintendência e Coordenação Técnica defina e formalize seus Fluxos Internos de Trabalho.

Estes fluxos específicos devem descrever a rotina operacional da equipe técnica a partir do momento em que o chamado é escalonado pela Central de Atendimento até a devolução da solução.

Os fluxos desenhados pelas Superintendências atuarão como "subprocessos" que se conectam ao fluxo principal.

Embora cada área técnica tenha autonomia para organizar sua triagem e distribuição de tarefas, todos os fluxos internos a serem anexados a este processo devem obrigatoriamente contemplar:

- Registro e Rastreabilidade Total;
    - Todos os incidentes devem ser tratados na ferramenta de Information Technology Service Management (ITSM), bem como ter seu histórico devidamente registrado.
- Consulta e Alimentação da Base de Conhecimento;
    - Durante investigação, a equipe de especialistas deve consultar a Base de Conhecimento, bem como ao solucionar um incidente, se a solução aplicada não estiver documentada ou for um erro novo, é dever da área técnica submeter a solução à Base de Conhecimento.
- Aderência ao SLA;
    - O fluxo interno de cada superintendência deve ser desenhado para que a solução ocorra dentro dos prazos de prioridades definidos.
- Recategorização;
    - É responsabilidade da equipe técnica corrigir a categorização do incidente caso a central de atendimento tenha classificado equivocadamente, garantindo a integridade dos relatórios gerenciais.

INCIDENTES GRAVES OPERACIONAIS E DE SEGURANÇA DA INFORMAÇÃO

Esta seção estabelece os procedimentos para o tratamento de incidentes de alta criticidade, distinguindo entre Incidentes Graves Operacionais (foco na continuidade do serviço) e Incidentes de Segurança da Informação (foco na proteção de dados e ativos).

São eventos que causam interrupção total ou degradação severa em serviços críticos da SEFAZ-RJ (ex: Sistemas de Arrecadação, Nota Fiscal Eletrônica, Link Principal de Dados), impactando diretamente a receita do Estado ou o atendimento ao cidadão.

O fluxo de tratamento obedece às seguintes etapas:

1. Detecção e Gatilho: Ação: A identificação ocorre pela Central de Atendimento, por meio de múltiplos chamados simultâneos, ou pelas ferramentas de Monitoramento, que sinalizam a parada crítica.

2. Classificação e Acionamento: A Central de Atendimento classifica o chamado com prioridade "Crítica" e aciona imediatamente o Gerente do Incidentes e os Coordenadores Técnicos das áreas envolvidas (Infraestrutura, Sistemas, Banco de Dados).

3. Mobilização: É instaurada a “Sala de Guerra” (física ou virtual), reunindo especialistas técnicos e decisores. O foco desta etapa é exclusivamente a restauração do serviço, postergando a análise da causa raiz para etapa posterior.

4. Comunicação: A SUBTIC deve emitir, tempestivamente, um comunicado de "Indisponibilidade Massiva" para usuários internos e externos, visando dar transparência.

5. Pós-Incidente: Após a estabilização, são obrigatórias as seguines ações:

    a. Elaboração do Relatório de Pós – Incidente, detalhando a linha do tempo, ações tomadas e impactos.

    b. Abertura de um registro do problema para análise de causa raiz, visando evitar a recorrência.

    c. Emissão de comunicado de restabelecimento de serviço, informando o retorno à normalidade aos usuários impactados.

Diferente dos incidentes operacionais, o tratamento de incidentes de Segurança tem foco nos pilares de Confidencialidade, Integridade e Disponibilidade sob a ótica de ameaças cibernéticas.

Devido à sua natureza sensível e à necessidade de preservação de evidências forenses, estes incidentes exigem ritos de contenção e erradicação que devem seguir o fluxo de Processo de Gestão de Incidentes de Segurança da Informação da SEFAZ/RJ.

Deve ser classificado como incidente grave de segurança da informação qualquer evento que envolva:

1. Vazamento ou Exfiltração de Dados: Suspeita ou confirmação de cópia não autorizada de dados sensíveis ou sigilosos (fiscais/tributários).

2. Comprometimento de Acesso: Acesso não autorizado a contas privilegiadas (Administradores, *root*) ou sistemas críticos.

3. Códigos Maliciosos (Malware/Ransomware): Infecção por softwares maliciosos com potencial de propagação lateral na rede ou criptografia de dados.

4. Ataques à Disponibilidade: Ataques de Negação de Serviço (*DDoS*) ou sabotagem deliberada de infraestrutura.

INDICADORES DE DESEMPENHO

O Gerente do Incidente é responsável por avaliar a qualidade e a efetividade do Gerenciamento de Incidentes por meio da mensuração dos indicadores de desempenho estabelecidos. Essa análise deve identificar desvios, oportunidades de melhoria e o grau de aderência às metas definidas. Deverá ser elaborado um relatório consolidando as métricas coletadas e a avaliação da qualidade do Processo de Gerenciamento de Incidentes.

Indicador	Fórmula	Periodicidade	Meta	Responsável
Percentual de incidentes resolvidos no prazo	Total de incidentes resolvidos no prazo/ Total de incidentes resolvidos	Anual	**≥ 80%**	Gerente do Incidente
Taxa de Resolução no primeiro Contato	Total de incidentes resolvidos na Central de Atendimento/ Total de incidentes resolvidos	Anual	**≥ 50%**	Gerente de Incidente

SISTEMÁTICA DE REVISÃO

O Processo de Gerenciamento de Incidentes deverá ser formalmente publicado, amplamente comunicado a todas as áreas da SUBTIC e mantido atualizado de forma sistemática. A revisão deve ocorrer, obrigatoriamente, com periodicidade mínima anual, ou antes disso, caso sejam identificadas mudanças que impactem os serviços prestados pela SEFAZ-RJ.

Ao final do fluxo de atualização, será emitida uma nova versão oficial do processo, com a devida atualização do controle de versões e o registro detalhado das alterações realizadas. A versão atualizada deverá ser amplamente divulgada a todas as áreas envolvidas, garantindo conhecimento, alinhamento e correta aplicação do processo revisado.

REFERÊNCIAS

[1] AXELOS. ITIL® Foundation: ITIL 4. London: The Stationery Office, 2019.

HISTÓRICO DE VERSÕES

Data	Versão	Alterações realizadas
15/12/2025	1.0	Criação do processo de gerenciamento de incidentes
07/01/2026	2.0	Aprimoramento do fluxo de incidentes

ANEXO

Fluxo Central de Atendimento