POLÍTICA DE GERENCIAMENTO DE INCIDENTES DE TIC

PODER JUDICIÁRIO
DO ESTADO DA BAHIA

Histórico de revisões

Data	Versão	Autoria	Descrição
18/03/2026	1.0	SETIM	Versão original do documento

Sumário

1 INTRODUÇÃO

A Política de Gerenciamento de Incidentes de Tecnologia da Informação e Comunicação (TIC) estabelece as diretrizes, papéis e responsabilidades para o tratamento adequado dos incidentes que afetem ou possam afetar os serviços de TIC no âmbito do Tribunal de Justiça do Estado da Bahia (TJBA).

Sob a perspectiva do Sistema de Valor do Serviço da Information Technology Infrastructure Library (ITIL), o Gerenciamento de Incidentes não se limita à execução de processos operacionais, mas integra o sistema de geração de valor institucional. Ao assegurar a rápida restauração dos serviços de TIC e a redução de indisponibilidades, essa prática contribui diretamente para a entrega de valor público, para o alcance dos objetivos estratégicos do Tribunal e para o fortalecimento da confiança dos usuários internos e externos na capacidade institucional de prover serviços digitais seguros, estáveis e eficientes.

O Gerenciamento de Incidentes tem como finalidade principal assegurar a rápida e eficaz restauração dos serviços de TIC, minimizando impactos às atividades institucionais, aos usuários e à prestação jurisdicional, bem como promovendo previsibilidade, padronização, rastreabilidade e transparência no atendimento das demandas relacionadas a incidentes.

Esta Política está alinhada às boas práticas de Gerenciamento de Serviços de TIC, notadamente à ITIL, em sua versão 4, bem como aos princípios de governança, gestão de riscos, continuidade do negócio e melhoria contínua adotados no setor público.

No contexto do TJBA, a Secretaria de Tecnologia e Modernização (SETIM) exerce um papel central na coordenação e na execução do Gerenciamento de Incidentes, atuando de forma integrada com as demais unidades, com o Service Desk, com os Grupos Solucionadores e com as equipes responsáveis por Segurança da Informação, Continuidade e Governança de TIC.

A Política abrange todas as etapas do ciclo de vida do incidente, desde sua identificação e registro até a completa restauração do serviço e o encerramento formal da ocorrência.

A efetividade desta Política contribui diretamente para a redução de indisponibilidades, para o aumento da confiabilidade dos serviços de TIC, para a melhoria da experiência dos usuários e para o fortalecimento da capacidade institucional do TJBA em suportar suas atividades finalísticas, assegurando uma prestação jurisdicional mais eficiente, contínua e alinhada aos objetivos estratégicos da Instituição.

CAPÍTULO I – DISPOSIÇÕES GERAIS

Esta Política estabelece as diretrizes, papéis e responsabilidades para o Gerenciamento de Incidentes relacionados aos serviços de TIC, no âmbito do TJBA, devendo ser observada por todas as unidades, magistrados, servidores, colaboradores e prestadores de serviços que atuem na utilização, suporte, operação ou gestão desses serviços.

O Gerenciamento de Incidentes deverá ser executado de forma padronizada, integrada e alinhada às boas práticas de Gerenciamento de Serviços de TIC, especialmente ao ITIL 4, bem como às políticas, normas e regulamentos institucionais vigentes.

A SETIM do TJBA é a unidade responsável pela implementação, gestão, monitoramento e comunicação das diretrizes estabelecidas nesta Política, sem prejuízo das atribuições das demais unidades envolvidas.

CAPÍTULO II – DAS DEFINIÇÕES E CONCEITOS

Para fins desta Política, adotam-se as seguintes definições:

I. Incidente: interrupção não planejada, redução da qualidade ou falha de um Serviço de TIC que possa resultar em impacto às atividades institucionais;

II. Incidente Grave: incidente que cause indisponibilidade significativa de serviços críticos, afete grande número de usuários, gere alto impacto institucional ou represente risco relevante à continuidade das atividades do TJBA;

III. Incidente de Segurança da Informação: toda ocorrência que afete ou possa afetar a confidencialidade, integridade ou disponibilidade das informações e dos serviços de TIC do TJBA, incluindo eventos decorrentes de falhas técnicas, humanas ou de ações intencionais, que representem risco às atividades institucionais, à continuidade do negócio ou ao cumprimento de obrigações legais e normativas;

IV. Solução de Contorno: medida temporária adotada para restaurar o serviço o mais rápido possível;

V. Restauração do Serviço: retorno do serviço ao seu nível normal de operação, conforme definido nos Acordos de Nível de Serviço;

VI. Escalonamento: encaminhamento do incidente para níveis técnicos ou hierárquicos superiores, quando necessário.

VII. Itens de Configuração (ICs): são componentes essenciais para a entrega eficiente e segura dos serviços de TIC. Eles incluem hardware, software, infraestrutura, documentação, dados, contratos e outras elementos que compõem um sistema ou serviço de TIC.

CAPÍTULO III – DOS OBJETIVOS

Esta Política tem por objetivo geral estabelecer diretrizes para o Gerenciamento de Incidentes, assegurando que esses eventos sejam devidamente registrados, classificados, analisados, priorizados, atendidos e concluídos de forma padronizada e tempestiva, com vistas à rápida restauração dos serviços de TIC afetados, à minimização dos impactos aos usuários e às atividades institucionais.

São objetivos específicos desta Política:

I. Padronizar a prática de Gerenciamento de Incidentes, em alinhamento às práticas do ITIL 4;

II. Assegurar que todos os incidentes sejam devidamente registrados, classificados, tratados, resolvidos e que as soluções sejam devidamente comunicadas às partes interessadas;

III. Assegurar que métodos e procedimentos padronizados sejam adotados para permitir uma resposta rápida e eficiente aos incidentes;

IV. Reduzir os impactos nas áreas de Negócio decorrentes de indisponibilidades não programadas dos serviços de TIC;

V. Alinhar as atividades do Gerenciamento de Incidentes às prioridades das áreas de Negócio;

VI. Manter e elevar o nível de satisfação dos usuários quanto à qualidade dos serviços de TIC.

VII. Orientar as partes interessadas e servir como instrumento corporativo de referência para o Gerenciamento de Incidentes no âmbito do TJBA.

CAPÍTULO IV - DO ESCOPO

Esta política aplica-se a todos os incidentes registrados, incluindo, mas não se limitando a:

I. Incidentes que causem interrupção total ou parcial dos serviços;
II. Incidentes que resultem em degradação de desempenho;
III. Incidentes relacionados a falhas em sistemas, infraestrutura, hardware, redes e aplicações;
IV. Incidentes de Segurança da Informação;
V. Incidentes Graves;

CAPÍTULO V – DOS PAPÉIS E RESPONSABILIDADES

Para fins desta Política, são definidos os seguintes papéis, com suas respectivas responsabilidades:

I. Usuário
a) Comunicar incidentes por meio dos canais oficiais do Service Desk;
b) Fornecer informações claras e completas sobre o incidente;
c) Validar a restauração do serviço, quando solicitado;
d) Responder à pesquisa instantânea de satisfação do Service Desk.

II. Service Desk (Primeiro Nível de Atendimento)
a) Atuar como ponto de contato com os usuários e demais partes afetadas pelos incidentes;
b) Registrar, classificar, priorizar, acompanhar e atualizar os incidentes na ferramenta corporativa de gestão de serviços;
c) Realizar o diagnóstico inicial e promover a resolução do incidente, sempre que possível, no primeiro nível de atendimento;
d) Identificar, declarar e acionar o fluxo específico para tratamento de Incidentes Graves, quando aplicável;

e) Comunicar, de forma clara e tempestiva, os usuários e as partes interessadas quanto ao status, impactos, previsão de restauração dos serviços e após a resolução de cada incidente;
f) Encerrar o incidente após a restauração do serviço, a devida validação e o registro das informações pertinentes.

III. Grupos Solucionadores (Segundo e Terceiro Níveis de Atendimento)

a) Atuar na investigação e resolução técnica dos incidentes;
b) Registrar e manter atualizadas todas as informações relativas ao incidente na ferramenta de gestão de serviços;
c) Cumprir os prazos, prioridades e níveis de serviço estabelecidos nos Acordos de Nível de Serviço (ANS).

IV. Fornecedores

a) Executar, apoiar e garantir o atendimento dos incidentes quando necessário;
b) Garantir a aderência ao Catálogo de Serviços de TIC, aos ANS e a esta Política;
c) Atuar como parceiro técnico-operacional.

V. Gestor da Prática de Gerenciamento de Incidentes de TIC

a) Monitorar o tratamento dos incidentes;
b) Coordenar o tratamento de Incidentes Graves;
c) Propor ações para a implementação de melhorias nos procedimentos e práticas relacionadas ao Gerenciamento de Incidentes.

VI. Equipe de Segurança da Informação (quando aplicável)

a) Atuar no tratamento de incidentes de Segurança da Informação;
b) Avaliar impactos, riscos e necessidade de comunicação institucional;
c) Apoiar ações de contenção, mitigação e prevenção.

CAPÍTULO VI – DAS INTERFACES COM OUTRAS PRÁTICAS

O Gerenciamento de Incidentes de TIC mantém interfaces diretas com as demais práticas de Gerenciamento de Serviços de TIC, conforme descrito a seguir:

I. Service Desk

Atua como ponto único de contato, sendo responsável pelo registro, classificação inicial, priorização, comunicação com os usuários, acompanhamento e encerramento dos incidentes, bem como pelo escalonamento aos Grupos Solucionadores quando necessário.

II. Gerenciamento de Problemas

Recebe informações provenientes de incidentes recorrentes ou de alto impacto, com o objetivo de identificar causas-raiz, propor soluções definitivas e reduzir a reincidência de incidentes no ambiente de TIC.

III. Gerenciamento de Configuração de Serviços de TIC

Garante que os ICs e seus relacionamentos estejam corretamente registrados e atualizados no Sistema de Gerenciamento de Configuração (SGC), apoiando a análise de impacto, o diagnóstico e a resolução de incidentes.

IV. Habilitação de Mudanças e Gerenciamento de Liberações

Sempre que a resolução de um incidente demandar a implementação de uma mudança, esta deverá ser registrada, avaliada, autorizada e implementada de forma controlada, mitigando riscos e evitando a introdução de novos incidentes no ambiente produtivo.

V. Monitoramento e Gerenciamento de Eventos

Contribui para a detecção contínua de eventos e condições anormais no ambiente de TIC, possibilitando a atuação preventiva ou corretiva,

com o objetivo de evitar a ocorrência de incidentes ou reduzir seus impactos aos serviços.

VI. Gerenciamento de Conhecimento

Apoia o Gerenciamento de Incidentes por meio da criação, manutenção e disseminação de uma base de conhecimento atualizada, contendo soluções conhecidas, procedimentos operacionais e soluções de contorno, contribuindo para a redução do tempo de atendimento e aumento da eficiência na resolução dos incidentes.

VII. Gerenciamento de Nível de Serviço

Responsável por definir, monitorar e revisar os ANS aplicáveis ao Gerenciamento de Incidentes, assegurando o cumprimento dos prazos de resposta e resolução acordados com as áreas de Negócio.

VIII. Gerenciamento do Catálogo de Serviços de TIC

Assegura que os serviços de TIC estejam devidamente definidos, categorizados e atualizados no Catálogo de Serviços de TIC, possibilitando a correta identificação dos serviços afetados por incidentes e a adequada priorização e tratamento conforme os níveis de serviço estabelecidos.

IX. Gerenciamento de Continuidade de Serviço

Assegura que os serviços de TIC possam ser recuperados e operados dentro de níveis previamente definidos após a ocorrência de Incidentes Graves, apoiando a continuidade do negócio e a mitigação de riscos institucionais.

CAPÍTULO VII – DAS DIRETRIZES

Seção I - Diretrizes sobre Registro e Identificação

Todos os incidentes de TIC deverão ser obrigatoriamente registrados, classificados, acompanhados e encerrados por meio da ferramenta oficial de

gestão de serviços adotada pelo TJBA, assegurando a rastreabilidade completa durante todo o seu ciclo de vida, desde a identificação até o encerramento.

O registro do incidente deverá conter, no mínimo, as seguintes informações:

I. Data e hora da identificação;
II. Serviço afetado;
III. Descrição clara e objetiva do incidente;
IV. Categoria;
V. Impactos percebidos;
VI. Usuários ou unidades afetadas

Incidentes identificados por ferramentas de monitoramento, automação, auditorias deverão ser registrados da mesma forma que os incidentes reportados pelos usuários, garantindo tratamento uniforme e padronizado;

Incidentes que representem risco à continuidade das atividades institucionais deverão ser tratados em consonância com as diretrizes de Continuidade e demais normativos do TJBA.

Incidentes de Segurança da Informação deverão ser tratados em consonância com práticas e normativos específicas.

Seção II - Diretrizes sobre Classificação e Priorização

Todos os incidentes deverão ser classificados de acordo com critérios previamente definidos, visando assegurar tratamento adequado, padronizado e proporcional ao impacto causado à Instituição.

A priorização dos incidentes deverá considerar, de forma combinada e justificada, os seguintes fatores:

I. Impacto ao Negócio, avaliando o grau de prejuízo às atividades institucionais;

II. Urgência, considerando o tempo aceitável para a restauração do serviço;

III. Quantidade de usuários afetados, direta ou indiretamente;

IV. Criticidade do serviço, conforme definido no Catálogo de Serviços de TIC;

V. Riscos à Segurança da Informação, incluindo confidencialidade, integridade e disponibilidade;

A priorização deverá ser realizada com base em matriz de priorização formalizada em normativo complementar a esta Política, observando critérios objetivos previamente estabelecidos

A priorização poderá ser revista ao longo do ciclo de vida do incidente, sempre que houver alteração no seu impacto ou contexto.

Seção III - Diretrizes sobre Atendimento e Resolução

O atendimento aos incidentes deverá observar fluxos, papéis e responsabilidades claramente definidos, garantindo agilidade, padronização e qualidade na prestação do serviço.

O atendimento e a resolução dos incidentes deverão considerar que:

I. O foco principal é a rápida restauração do serviço, minimizando impactos às atividades institucionais;

II. Sempre que necessário, soluções de contorno poderão ser adotadas com o objetivo de restabelecer o serviço no menor tempo possível;

III. As soluções definitivas para a causa-raiz do incidente poderão ser tratadas por meio da prática de Gerenciamento de Problemas;

IV. A comunicação com os usuários afetados deverá ser clara, objetiva e contínua, especialmente em incidentes de maior impacto.

Seção IV - Diretrizes sobre Escalonamento

O escalonamento dos incidentes deverá ocorrer sempre que a resolução não puder ser realizada no nível inicial de atendimento ou quando houver risco de descumprimento dos níveis de serviço estabelecidos.

I. O escalonamento funcional deverá ser realizado para os Grupos Solucionadores responsáveis, conforme a natureza técnica do incidente;
II. O escalonamento hierárquico deverá ser adotado quando houver impacto relevante às atividades institucionais, necessidade de decisão gerencial ou caracterização de Incidente Grave.

Seção V - Diretrizes sobre Comunicação com Usuários e Partes Interessadas

A comunicação relacionada aos incidentes deverá ser realizada de forma clara, objetiva, tempestiva e por canais oficiais.

I. Em Incidentes Graves, deverão ser prestadas informações periódicas sobre status, impactos e previsão de restauração.
II. A comunicação institucional deverá observar as orientações da gestão e os normativos internos vigentes.

Seção VI - Diretrizes sobre Encerramento de Incidentes

O encerramento de um incidente somente poderá ocorrer após:

I. A efetiva restauração do serviço afetado;
II. A validação da solução, quando aplicável, junto ao usuário ou unidade demandante;

III. O registro completo da solução adotada, da classificação final e das informações relevantes para fins de histórico e auditoria;
IV. O encerramento inadequado de incidentes será tratado como não conformidade processual.

Seção VII - Diretrizes sobre Incidentes Graves

Os Incidentes Graves, assim definidos conforme critérios estabelecidos pela Instituição, deverão receber tratamento diferenciado, observando-se as seguintes diretrizes:

I. Devem seguir fluxo específico, prioritário e previamente definido;
II. Devem contar com coordenação centralizada, assegurando tomada de decisão rápida e alinhada;
III. Exigem comunicação contínua e estruturada às partes interessadas, incluindo áreas técnicas, gestão e usuários afetados;
IV. Devem ser objeto de análise pós-incidente, visando identificar causas, impactos, ações corretivas e lições aprendidas;
V. As lições aprendidas deverão subsidiar melhorias nos processos, controles e serviços de TIC.

Seção VIII - Diretrizes sobre Incidentes de Segurança da Informação

Os Incidentes de Segurança da Informação deverão ser tratados com prioridade e rigor, observando-se as seguintes diretrizes:

I. Devem ser imediatamente comunicados à equipe responsável por Segurança da Informação;
II. Devem observar integralmente a Política de Segurança da Informação, bem como normas e legislações aplicáveis;

III. Podem exigir a adoção de ações de contenção, isolamento, mitigação e erradicação do incidente;
IV. Poderão demandar comunicação institucional, quando aplicável, conforme diretrizes da alta administração;
V. Devem ser registrados e documentados de forma detalhada para fins de auditoria e melhoria contínua.

Seção IX - Diretrizes sobre Base de Conhecimento e Melhoria Contínua

As soluções aplicadas aos incidentes, especialmente aquelas recorrentes ou de alto impacto, deverão ser registradas na Base de Conhecimento institucional.

I. A Base de Conhecimento deverá ser utilizada como fonte prioritária para resolução de incidentes similares;
II. As informações registradas deverão subsidiar ações de melhoria contínua, revisão de procedimentos e capacitação das equipes.

Seção X - Diretrizes sobre Níveis de Serviço e Monitoramento e Automação

No que se refere aos níveis de serviço, monitoramento e à automação no gerenciamento de incidentes, deverão ser observadas as seguintes diretrizes:

I. Os incidentes deverão ser atendidos em conformidade com os ANS estabelecidos, priorizando a restauração célere dos serviços;
II. Os níveis de serviço deverão considerar a criticidade e a prioridade do incidente, podendo variar de acordo com sua classificação.
III. O acompanhamento e o monitoramento das tratativas serão realizados pelo pessoal do Service Desk e pelos gestores responsáveis, quando for o caso;

IV. Os indicadores de desempenho, tais como tempo de atendimento, tempo de resolução, tempo de detecção, cumprimento de prazos e de ANSs, satisfação do usuário, taxa de reincidência, percentual de resolução no primeiro nível e tempo médio para declaração de Incidente Grave, deverão ser coletados, analisados e reportados periodicamente;

V. Os resultados dos indicadores deverão subsidiar ações de melhoria contínua nos processos e serviços de TIC;

VI. Sempre que tecnicamente viável e estrategicamente alinhado aos objetivos institucionais, deverão ser adotados mecanismos de automação, incluindo monitoramento proativo, abertura automática de incidentes a partir de eventos identificados por ferramentas de supervisão, soluções de autoatendimento ao usuário e utilização de recursos de inteligência artificial para apoio à detecção, correlação, classificação e priorização de incidentes.

Seção XI - Diretrizes sobre Conformidade

Esta Política deve estar alinhada e em conformidade com:

I. Política da Central de Serviços, Requisições de Serviços de TIC e Gerenciamento de Problemas;

II. Política de Governança de TIC;

III. Política de Segurança da Informação;

IV. Os atos normativos e regulamentações aplicáveis;

V. O descumprimento das diretrizes estabelecidas será tratado como não conformidade, sujeito às medidas administrativas cabíveis.

2 DISPOSIÇÕES FINAIS

As situações não previstas nesta Política, bem como eventuais dúvidas quanto à sua aplicação, deverão ser analisadas e dirimidas pela SETIM, observadas as normas institucionais, os princípios da Governança de TIC e as boas práticas de Gerenciamento de Serviços.

Os procedimentos operacionais, fluxos de atendimento, critérios de classificação, priorização e escalonamento de incidentes poderão ser detalhados em normativos complementares, manuais, instruções normativas ou documentos técnicos específicos, desde que em consonância com as diretrizes estabelecidas nesta Política.

A implementação e a observância desta Política não eximem as unidades, servidores, colaboradores e prestadores de serviços do cumprimento das demais normas internas, políticas institucionais e legislações aplicáveis, especialmente aquelas relacionadas à Segurança da Informação, à proteção de dados pessoais, à Continuidade e à governança pública.

Esta Política deverá ser amplamente divulgada no âmbito do TJBA, cabendo às unidades gestoras promover ações de comunicação, capacitação e conscientização, de forma a assegurar seu adequado entendimento, aplicação e efetividade.

Os resultados obtidos a partir da aplicação desta Política, bem como os indicadores, análises e lições aprendidas decorrentes do Gerenciamento de Incidentes, deverão subsidiar ações de melhoria contínua dos processos, dos serviços de TIC e do modelo de governança adotado pelo Tribunal.