DJEN Bahia
Disponibilização: 18/08/2026
Publicação: 18/08/2026

PORTARIA SETIM N. 63/2026

Institui a Política de Gerenciamento de Incidentes de Tecnologia da Informação e Comunicação no âmbito do Tribunal de Justiça do Estado da Bahia.

O SECRETÁRIO DE TECNOLOGIA DA INFORMAÇÃO E MODERNIZAÇÃO DO TRIBUNAL DE JUSTIÇA DO ESTADO DA BAHIA, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de fortalecimento da governança de Tecnologia da Informação e Comunicação (TIC) no âmbito do Tribunal de Justiça do Estado da Bahia (TJBA);

CONSIDERANDO que a crescente dependência dos serviços de TIC exige mecanismos eficazes para prevenção, identificação, tratamento e resolução de incidentes que possam impactar a continuidade das atividades institucionais;

CONSIDERANDO a importância de estabelecer diretrizes claras, padronizadas e transparentes para o registro, a classificação, a priorização, o atendimento, a comunicação e o encerramento de incidentes de Tecnologia da Informação e Comunicação;

CONSIDERANDO a adoção das boas práticas de Gerenciamento de Serviços de TIC, em especial aquelas preconizadas pela ITIL 4, com foco na rápida restauração dos serviços, na jornada do usuário, na cadeia de valor institucional e na cocriação de valor;

CONSIDERANDO a necessidade de promover a eficiência operacional, a padronização de procedimentos, a automação de processos, a transparência e a rastreabilidade ao longo do ciclo de vida dos incidentes de TIC;

CONSIDERANDO a relevância do tratamento prioritário e estruturado dos Incidentes Graves e dos Incidentes de Segurança da Informação, em observância às diretrizes institucionais, às normas vigentes e à proteção das informações e serviços críticos;

CONSIDERANDO o contido no expediente SEI n. 80521052.000062/2026-77;

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Gerenciamento de Incidentes de Tecnologia da Informação e Comunicação (TIC) no âmbito do Tribunal de Justiça do Estado da Bahia.

§ 1º A 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.

§ 2º O Gerenciamento de Incidentes de TIC deverá ser executado de forma

padronizada, integrada e alinhada às boas práticas de Gerenciamento de Serviços de TIC, especialmente à ITIL 4, bem como às políticas, normas e regulamentos institucionais vigentes.

Art. 2º A Secretaria de Tecnologia da Informação e Modernização (SETIM) 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

Art. 3º Para fins desta Política, adotam-se as seguintes definições:

I. Incidente de TIC: 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: evento ou conjunto de eventos indesejados que comprometem, ou têm potencial para comprometer, a confidencialidade, integridade ou disponibilidade das informações e dos ativos de informação de uma organização;

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 (ANS);

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

VII. Fornecedor de TIC: pessoa física ou jurídica, pública ou privada, contratada ou conveniada ao Tribunal de Justiça do Estado da Bahia, responsável pelo fornecimento de bens, soluções, sistemas, serviços, suporte técnico, manutenção, infraestrutura ou quaisquer outros recursos de Tecnologia da Informação e Comunicação, que participe direta ou indiretamente da operação, sustentação ou recuperação dos serviços de TIC;

VIII. Equipe de Segurança da Informação: equipe composta pela Assessoria de Segurança da Informação e pelos técnicos envolvidos na solução dos incidentes de segurança da informação;

IX. Itens de Configuração (ICs): componentes que integram a entrega dos serviços de TIC, incluindo hardware, software, infraestrutura, documentação, dados, contratos e demais elementos que compõem um sistema ou serviço de TIC.

CAPÍTULO III
DOS OBJETIVOS

Art. 4º Esta Política tem por objetivo geral estabelecer diretrizes para o Gerenciamento de Incidentes de TIC, 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 e à minimização dos impactos aos usuários e às atividades institucionais.

Art. 5º São objetivos específicos desta Política:

I. padronizar a prática de Gerenciamento de Incidentes de TIC, em alinhamento às práticas da ITIL 4;

II. assegurar que todos os incidentes sejam devidamente registrados, classificados, tratados e 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 de TIC às prioridades das áreas de negócio;

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

CAPÍTULO IV
DO ESCOPO

Art. 6º Esta Política aplica-se a todos os incidentes de TIC, incluindo, mas não se limitando a:

I. incidentes que causem interrupção total ou parcial dos serviços de TIC;

II. incidentes que resultem em degradação de desempenho dos serviços de TIC;

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

Art. 7º 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 a status, impactos e previsão de restauração dos serviços, bem como após a resolução de cada incidente;

f) encerrar o chamado após a restauração do serviço, a devida validação e o registro das informações pertinentes.

III. Grupo Solucionador (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 ANS.

IV. Fornecedor de TIC:

a) comunicar imediatamente ao TJBA a ocorrência ou suspeita de incidentes relacionados aos serviços, sistemas, soluções ou recursos de TIC sob sua responsabilidade;

b) atuar na identificação, análise, contenção, tratamento e resolução dos incidentes relacionados aos serviços ou ativos de TIC de sua competência, observados os níveis de serviço estabelecidos contratualmente;

c) prestar suporte técnico às equipes do TJBA durante as atividades de investigação, resposta, recuperação e restauração dos serviços afetados por incidentes;

d) fornecer informações, evidências, registros, logs, relatórios e demais subsídios necessários à análise, tratamento e apuração dos incidentes.

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

Art. 8º 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 o 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

Art. 9º 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.

Parágrafo único. 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.

Art. 10 Incidentes identificados por ferramentas de monitoramento, automação ou auditorias deverão ser registrados da mesma forma que os incidentes reportados pelos usuários, garantindo tratamento uniforme e padronizado.

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

Art. 11 Incidentes de Segurança da Informação deverão ser tratados em consonância com práticas e normativos específicos.

Seção II
Diretrizes sobre Classificação e Priorização

Art. 12 Todos os incidentes deverão ser classificados de acordo com critérios previamente definidos, visando assegurar tratamento adequado, padronizado e proporcional ao impacto causado à instituição.

Parágrafo único. 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.

Art. 13 A priorização deverá ser realizada com base em matriz de priorização formalizada em normativo complementar a esta Política, observando critérios objetivos previamente estabelecidos.

Parágrafo único. 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

Art. 14 O atendimento aos incidentes deverá observar fluxos, papéis e responsabilidades claramente definidos, garantindo agilidade, padronização e qualidade na prestação do serviço.

Parágrafo único. 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

Art. 15 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.

§ 1º O escalonamento funcional deverá ser realizado para os Grupos Solucionadores responsáveis, conforme a natureza técnica do incidente.

§ 2º 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

Art. 16 A comunicação relacionada aos incidentes deverá ser realizada de forma clara, objetiva, tempestiva e por canais oficiais.

§ 1º Em Incidentes Graves, deverão ser prestadas informações periódicas sobre status, impactos e previsão de restauração.

§ 2º A comunicação institucional deverá observar as orientações da gestão e os normativos internos vigentes.

Seção VI
Diretrizes sobre Encerramento de Incidentes

Art. 17 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.

Parágrafo único. O encerramento inadequado de incidentes será tratado como não conformidade processual.

Seção VII
Diretrizes sobre Incidentes Graves

Art. 18 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

Art. 19 Os Incidentes de Segurança da Informação, incluindo aqueles relacionados à proteção de dados pessoais, nos termos da legislação aplicável, 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.

§ 1º O tratamento de Incidentes de Segurança da Informação deverá observar procedimentos específicos de segurança, formalizados em normativos complementares, sendo de responsabilidade da Equipe de Tratamento e Resposta a Incidentes (ETIR) a condução das ações técnicas de resposta, contenção, erradicação e recuperação, em conformidade com as diretrizes estabelecidas pelo Colegiado de Segurança da Informação do TJBA.

§ 2º O Colegiado de Segurança da Informação é o órgão responsável pela deliberação sobre as diretrizes, prioridades e medidas estratégicas relacionadas ao tratamento de Incidentes de Segurança da Informação, cabendo-lhe orientar e supervisionar as ações da ETIR, avaliar os impactos institucionais e determinar, quando necessário, a adoção de medidas excepcionais de proteção e resposta.

Seção IX
Diretrizes sobre Base de Conhecimento e Melhoria Contínua

Art. 20 As soluções aplicadas aos incidentes, especialmente aquelas recorrentes ou de alto impacto, deverão ser registradas na Base de Conhecimento institucional.

§ 1º A Base de Conhecimento deverá ser utilizada como fonte prioritária para resolução de incidentes similares.

§ 2º As informações registradas deverão subsidiar ações de melhoria contínua, revisão de procedimentos e capacitação das equipes.

Seção X
Diretrizes sobre Níveis de Serviço, Monitoramento e Automação

Art. 21 No que se refere aos níveis de serviço, ao 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 ANS, 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

Art. 22 Esta Política deve estar alinhada e em conformidade com:

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

II. a Política de Governança de TIC;

III. a Política de Segurança da Informação;

IV. os atos normativos e regulamentações aplicáveis.

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

CAPÍTULO XII
DAS DISPOSIÇÕES FINAIS

Art. 23 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.

Art. 24 Esta Política deverá ser revisada, no mínimo, a cada 2 (dois) anos ou sempre que houver alteração relevante no arcabouço legal ou tecnológico.

Art. 25 Esta Portaria entra em vigor na data da sua publicação.

Salvador, *data da assinatura eletrônica.*

Leonardo de Andrade Ferraz Fogaça
Secretário de Tecnologia da Informação e Modernização

Documento assinado eletronicamente por **Leonardo de Andrade Ferraz Fogaça**, **Secretário(a) de Tecnologia da Informação e Modernização**, em 14/08/2026, às 16:55, conforme horário oficial de Brasília, com fundamento no art. 6º do Decreto nº 8.539, de 8 de outubro de 2015.