Universidade Estadual de Londrina

LUIZ CARLOS GARANHANI JUNIOR

GAIA-MGE:

UM MODELO PARA MONITORAÇÃO E GERENCIAMENTO DE EVENTOS BASEADO EM ITIL 4, PARA UMA INSTITUIÇÃO PÚBLICA MUNICIPAL

Londrina
2026

LUIZ CARLOS GARANHANI JUNIOR

GAIA-MGE:
UM MODELO PARA MONITORAÇÃO E GERENCIAMENTO DE EVENTOS BASEADO EM ITIL 4, PARA UMA INSTITUIÇÃO PÚBLICA MUNICIPAL

Dissertação apresentado ao Curso de Mestrado em Ciência da Computação do Departamento de Computação da Universidade Estadual de Londrina, como requisito parcial para a obtenção do título de Mestre em Ciência da Computação.

Orientador: Prof. Dr. Rodolfo Miranda de Barros.

Londrina
2026

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema de Bibliotecas da UEL

G212g Garanhani Junior, Luiz Carlos.
GAIA-MGE: um modelo para monitoração e gerenciamento de eventos baseado em ITIL 4, para uma instituição pública municipal / Luiz Carlos Garanhani Junior. - Londrina, 2026.
174 f. : il.

Orientador: Rodolfo Miranda de Barros. Coorientador: Vanessa Tavares de Oliveira Barros. Coorientador: Lourival Aparecido de Góis. Dissertação (Mestrado em Ciência da Computação) - Universidade Estadual de Londrina, Centro de Ciências Exatas, Programa de Pós-Graduação em Ciência da Computação, 2026.
Inclui bibliografia.

1. Monitoração e Gerenciamento de Eventos - Tese. 2. ITIL 4 - Tese. 3. Lógica Fuzzy - Tese. 4. Automação de Serviços Públicos - Tese. I. Miranda de Barros, Rodolfo. II. Tavares de Oliveira Barros, Vanessa. III. Aparecido de Góis, Lourival. IV. Universidade Estadual de Londrina. Centro de Ciências Exatas. Programa de Pós-Graduação em Ciência da Computação. V. Título.

CDU 519

LUIZ CARLOS GARANHANI JUNIOR

GAIA-MGE:
UM MODELO PARA MONITORAÇÃO E GERENCIAMENTO DE EVENTOS BASEADO EM ITIL 4, PARA UMA INSTITUIÇÃO PÚBLICA MUNICIPAL

Dissertação apresentada ao programa de Mestrado em Ciência da Computação do Departamento de Computação da Universidade Estadual de Londrina, como requisito parcial para obtenção do título de Mestre em Ciência da Computação.

BANCA EXAMINADORA

Orientador: Prof. Dr. Rodolfo Miranda de Barros
Universidade Estadual de Londrina - UEL

Profa. Dra. Vanessa Tavares de Oliveira Barros
Universidade Estadual de Londrina - UEL

Prof. Dr. Lourival Aparecido de Góis
Universidade Tecnológica Federal do Paraná - UTFPR

Londrina, 31 de março de 2026.

Dedico este trabalho à minha esposa, meu amor, porto seguro e pilar fundamental da nossa família. Sua compreensão, incentivo e companheirismo foram fundamentais em cada etapa desta jornada. À minha esposa, agradeço por compartilhar comigo os desafios e conquistas, oferecendo sempre apoio incondicional, amor e inspiração para seguir adiante.

Ao meu filho, razão do meu orgulho e motivação diária, dedico não apenas estas páginas, mas também o exemplo de perseverança, resiliência, ética e busca pelo conhecimento. Que esta conquista possa inspirá-lo a perseguir seus próprios sonhos com coragem, integridade e determinação.

AGRADECIMENTOS

Agradeço primeiramente a Deus por me conceder saúde, discernimento e força nos momentos mais desafiadores, iluminando meu caminho e fortalecendo minha fé ao longo desta caminhada.

À minha esposa *Priscila Eva Goldin de Andrade Garanhani*, expresso minha eterna gratidão pelo amor, compreensão, incentivo e parceria inabalável. Sua dedicação diária, capacidade de me apoiar mesmo diante das maiores dificuldades e sua paciência nas ausências impostas pelos estudos foram indispensáveis para a realização deste sonho. Sem sua presença constante, coragem e generosidade, esta conquista não teria sido possível.

Ao meu filho *Joaquim Goldin Garanhani*, minha fonte diária de inspiração, alegria e orgulho, agradeço profundamente por sua compreensão e carinho, mesmo sendo ainda tão pequeno. Em muitos momentos, você, com seu coração generoso, entendeu quando precisei priorizar os estudos em vez de brincar ou estar ao seu lado. As suas palavras doces, como tantas vezes ouvi: *"tudo bem papai, eu espero"*, a sua paciência infantil, os olhares curiosos e os abraços depois de um dia cansativo foram combustível para minha perseverança, tornando esta conquista ainda mais significativa. Que este trabalho, muitas vezes construído ao som das suas brincadeiras, inspire você a nunca desistir dos próprios sonhos e a buscar sempre o conhecimento, com a mesma alegria e curiosidade que demonstra a cada nova descoberta.

Aos meus pais, *Luiz Carlos Garanhani* e *Maria de Lourdes Marquezin Garanhani*, pelo exemplo de trabalho, honestidade e dedicação, e por sempre acreditarem no meu potencial. Seu apoio e ensinamentos foram e sempre serão a base de todas as minhas conquistas.

Ao meu orientador, *Prof. Dr. Rodolfo Miranda de Barros*, registro minha profunda gratidão pela orientação segura, pela confiança no meu trabalho e pelo incentivo contínuo ao longo desta pesquisa. Suas contribuições acadêmicas e críticas construtivas foram fundamentais para o amadurecimento científico deste estudo, assim como para meu desenvolvimento intelectual e profissional durante toda a trajetória.

À *Prof.ª Dr.ª Vanessa Tavares de Oliveira Barros*, registro minha sincera gratidão pela orientação dedicada e pelas contribuições fundamentais ao meu percurso acadêmico. Seu compromisso com o ensino e a pesquisa, assim como sua habilidade em promover o desenvolvimento intelectual e humano dos alunos, enriqueceram profundamente minha formação. A atenção e o apoio oferecidos ao longo da disciplina e nas discussões sobre os desafios da Administração Pública foram essenciais para o amadurecimento deste trabalho.

Aos colegas *Vagner Mantovani* e *Moisés de Sousa Galian*, pelo companheirismo, troca de experiências e incentivo durante a trajetória do mestrado, agradeço pela parceria constante, pelo apoio mútuo diante dos desafios e pela colaboração nas discussões acadêmicas e práticas. A convivência, o diálogo aberto e a disposição para compartilhar conhecimentos foram fundamentais para tornar essa jornada mais produtiva, enriquecedora e gratificante.

À Prefeitura Municipal de Arapongas, pelo apoio institucional, infraestrutura e oportunidade de aplicação prática do conhecimento adquirido, viabilizando a realização deste estudo em um contexto real.

À Universidade Estadual de Londrina (UEL), pela excelência acadêmica, corpo docente qualificado e ambiente de estímulo ao desenvolvimento científico, que permitiram o crescimento profissional e pessoal ao longo desta jornada.

Agradeço, ainda, a todos que, de alguma maneira, contribuíram para a concretização deste sonho. A realização deste trabalho representa uma conquista significativa em minha trajetória pessoal e profissional, fruto da dedicação, perseverança e do apoio generoso daqueles que estiveram ao meu lado em cada etapa deste percurso.

“Educação não transforma o mundo.
Educação muda as pessoas. Pessoas
transformam o mundo.”
(Paulo Freire, Educação e mudança)

RESUMO

GARANHANI JUNIOR, L. C. **GAIA-MGE:** um modelo para monitoração e gerenciamento de eventos baseado em ITIL 4, para uma instituição pública municipal. 174 p. Trabalho de Conclusão de Curso (Mestre em Ciência da Computação) – Universidade Estadual de Londrina, Londrina, 2026.

A transformação digital nos municípios brasileiros ampliou a dependência de serviços públicos digitais e elevou a complexidade das infraestruturas de Tecnologia da Informação e Comunicação (TIC), tornando mais crítica a necessidade de continuidade, confiabilidade e resposta tempestiva a falhas operacionais. Problema Científico e/ou Prático: A ausência de um fluxo automatizado de Monitoração e Gerenciamento de Eventos prolonga o Tempo Médio de Detecção (MTTD) e o Tempo Médio de Resolução (MTTR), comprometendo os Acordos de Nível de Serviço (SLAs) e a confiança do cidadão. Solução e/ou Análise Proposta: Esta pesquisa propõe uma arquitetura open source integrada, alinhada ao Gerenciamento de Eventos da ITIL 4 [1], composta pelo Zabbix, responsável pela detecção dos eventos, por um mecanismo de inferência Fuzzy desenvolvido em Python, voltado à classificação adaptativa de criticidade com base em impacto e urgência, e pelo GLPI, utilizado para o gerenciamento automatizado do ciclo de vida dos tickets. A lógica Fuzzy substitui limiares rígidos por avaliação contínua, enquanto mecanismos de idempotência evitam a abertura de tickets duplicados. Teoria de SI Relacionada: O artefato fundamenta-se no gerenciamento de serviços da ITIL 4 [1], na teoria dos conjuntos Fuzzy [2], [3], [4], e no paradigma de Design Science Research (DSR), conforme formalizado por [5] e [6]. Método de Pesquisa: O estudo seguiu as seis etapas da DSR: identificação do problema, definição dos objetivos, design e desenvolvimento, demonstração, avaliação e comunicação do artefato. A validação foi conduzida em ambiente piloto, segregado, porém alimentado com dados reais da infraestrutura de um órgão público municipal. Resumo dos Resultados: Os resultados evidenciaram a viabilidade técnica da automação ponta a ponta, com redução do intervalo entre a detecção do evento e a abertura do ticket para menos de um minuto, prevenção de duplicidades por idempotência, encerramento automático após a recuperação do evento e manutenção da rastreabilidade integral do processo. Contribuições e Impacto na Área de SI: O trabalho oferece um modelo replicável e de baixo custo para o setor público, apresenta evidências empíricas de que a priorização Fuzzy amplia a granularidade decisória na gestão de eventos e demonstra a viabilidade da integração entre governança orientada pela ITIL 4 [1] e orquestração automatizada por APIs REST. Ressalta-se, contudo, que a avaliação empírica da implantação automatizada foi realizada em escopo piloto, com quantidade restrita de ativos monitorados, o que limita a generalização dos resultados observados. Permanecem desafios estruturais relacionados à consolidação da Configuration Management Database (CMDB) e ao esforço inicial de parametrização dos ativos, etapas que demandam maturidade institucional e governança contínua. Além disso, o modelo ainda não contempla rotinas automáticas de ajuste das funções de pertinência, cuja implementação futura poderá ampliar sua capacidade adaptativa e sua precisão operacional.

Palavras-chave: Monitoração e Gerenciamento de Eventos; ITIL 4; Zabbix; Lógica Fuzzy; GLPI; Automação de Serviços Públicos; Governança de TIC.

ABSTRACT

GARANHANI JUNIOR, L. C. **GAIA-MGE:** a model for event monitoring and management based on ITIL 4, for a municipal public institution.174p. Final Project (Mater of Science in Computer Science) – State University of Londrina, Londrina, 2026.

The digital transformation in Brazilian municipalities has increased the dependence on digital public services and raised the complexity of Information and Communication Technology (ICT) infrastructures, making the need for continuity, reliability, and timely response to operational failures more critical. Scientific and/or Practical Problem: The absence of an automated Event Monitoring and Management flow prolongs the Mean Time To Detect (MTTD) and Mean Time To Resolve (MTTR), compromising Service Level Agreements (SLAs) and citizen trust. Proposed Solution and/or Analysis: This research proposes an integrated open-source architecture, aligned with ITIL 4 Event Management [1], composed of Zabbix, responsible for event detection, a Fuzzy inference mechanism developed in Python, focused on adaptive criticality classification based on impact and urgency, and GLPI, used for automated ticket lifecycle management. Fuzzy logic replaces rigid thresholds with continuous evaluation, while idempotency mechanisms prevent the opening of duplicate tickets. Related IS Theory: The artifact is based on ITIL 4 service management [1], Fuzzy set theory [2], [3], [4] and the Design Science Research (DSR) paradigm, as formalized by [5] and [6]. Research Method: The study followed the six stages of DSR: problem identification, definition of objectives, design and development, demonstration, evaluation, and communication of the artifact. Validation was conducted in a segregated pilot environment, but fed with real data from the infrastructure of a municipal public body. Summary of Results: The results demonstrated the technical feasibility of end-to-end automation, with a reduction in the interval between event detection and ticket opening to less than one minute, prevention of duplications due to idempotency, automatic closure after event recovery, and maintenance of full process traceability. Contributions and Impact in the IT Area: This work offers a replicable and low-cost model for the public sector, presents empirical evidence that Fuzzy prioritization increases decisional granularity in event management, and demonstrates the feasibility of integrating governance guided by ITIL 4 [1] and automated orchestration via REST APIs. It should be noted, however, that the empirical evaluation of the automated implementation was carried out in a pilot scope, with a limited number of monitored assets, which limits the generalization of the observed results. Structural challenges remain related to the consolidation of the Configuration Management Database (CMDB) and the initial effort of parameterizing the assets, steps that demand institutional maturity and continuous governance. Furthermore, the model does not yet include automatic routines for adjusting the relevance functions, whose future implementation could increase its adaptive capacity and operational accuracy.

Key-words: Event Monitoring and Management; ITIL 4; Zabbix; Fuzzy Logic; GLPI; Public Service Automation; ICT Governance.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AIOps	Artificial Intelligence for IT Operations
API	Interface de Programação de Aplicações (Application Programming Interface)
COBIT	Control Objectives for Information and Related Technology
BPMN	Business Process Model and Notation
CMDB	Configuration Management Database
COBIT	Control Objectives for Information and Related Technology
DMN	Decision Model and Notation
DTI	Diretoria de Tecnologia da Informação
DSR	Design Science Research
FM	Fator Multiplicativo
GLPI	Gestionnaire Libre de Parc Informatique
HTTP	Hypertext Transfer Protocol
IA	Inteligência Artificial
IC	Item de Configuração
IoT	Internet of Things
ITIL	Information Technology Infrastructure Library
ITSM	IT Service Management
IPMI	Intelligent Platform Management Interface
JMX	Java Management Extensions
JSON	JavaScript Object Notation
KPI	Key Performance Indicator
LF	Lógica Fuzzy
LSTM	Long Short-Term Memory
MFMC	Matriz Fuzzy Multicritério
MGE	Monitoração e Gerenciamento de Eventos
MTTD	Mean Time to Detect
MTTR	Mean Time to Repair
MIF	Motor de Inferência Fuzzy
ML	Machine Learning
NLP	Natural Language Processing
NMS	Network Management System

POP	Procedimento Operacional Padrão
QDA	Questionário de Diagnóstico de Avaliação
REST	Representational State Transfer
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol

SUMÁRIO

1 INTRODUÇÃO

A expansão acelerada das tecnologias digitais tem transformado profundamente as interações entre indivíduos, organizações e governos [7]. No setor público, tais avanços têm se refletido em ganhos expressivos de conveniência, acessibilidade e eficiência na prestação de serviços à sociedade [8].

À medida que as infraestruturas digitais se expandem, também se intensificam sua complexidade, sua interdependência e sua criticidade operacional, exigindo níveis cada vez mais elevados de disponibilidade, confiabilidade e capacidade de resposta [9]. Nesse cenário, a monitoração automatizada torna-se elemento estratégico para mitigar impactos operacionais, reduzir custos associados à indisponibilidade e sustentar a continuidade dos serviços [10].

No contexto brasileiro, esse desafio mostra-se particularmente relevante na esfera municipal. Embora 94% das prefeituras tenham registrado crescimento na demanda por serviços digitais após a pandemia de Covid-19, a integração entre sistemas ainda é considerada deficiente em 18% delas, comprometendo a eficiência administrativa e a continuidade dos serviços ofertados [11].

Essa expansão, muitas vezes conduzida de forma incremental e sob restrições orçamentárias e institucionais, somada à morosidade dos processos de aquisição e à ausência de planejamento estratégico consolidado, contribui para a fragmentação do ambiente tecnológico e para o aumento da vulnerabilidade operacional [12] [13]. Como consequência, reforça-se a necessidade de soluções integradas de governança, monitoração e tratamento de eventos em ambientes públicos cada vez mais dependentes da TIC.

Nesse contexto, a literatura aponta que a adoção de *frameworks* consolidados de gerenciamento de serviços, como o ITIL 4, pode contribuir para elevar a eficiência, a qualidade e a confiabilidade dos serviços de TI [14]. No entanto, revisões recentes indicam que ainda há carência de arquiteturas unificadas capazes de abranger, de forma integrada, todo o ciclo de monitoração, classificação inteligente de criticidade e gestão de *tickets* [15].

Essa lacuna se torna ainda mais crítica no contexto municipal, em que equipes de TI costumam operar com recursos humanos e orçamentários limitados, ao mesmo tempo em que precisam sustentar serviços digitais essenciais à administração

pública. Nesses ambientes, a ausência de modelos integrados de MGE tende a ampliar o tempo de detecção e resposta a incidentes, reduzindo a capacidade institucional de reação diante de falhas e degradações de serviço [16].

Evidências empíricas recentes indicam que o ITIL 4 oferece um arcabouço metodológico relevante para estruturar processos, antecipar falhas e alinhar as ações de Tecnologia da Informação e Comunicação (TIC) à missão institucional, fortalecendo a robustez operacional e a geração de valor [17]. Seu enfoque em criação de valor, melhoria contínua e integração entre práticas operacionais o torna especialmente pertinente para contextos organizacionais que demandam maior padronização e governança [1]

Além disso, estudos apontam o uso recorrente do ITIL e do COBIT em iniciativas de governança de TIC no setor público, evidenciando sua relevância para o aprimoramento da qualidade dos serviços digitais e para o fortalecimento dos mecanismos de controle, coordenação e alinhamento estratégico [18] [19]. Em ambientes públicos, tais referenciais também têm sido associados a ganhos de transparência, qualidade e maturidade institucional [20].

A prática de Monitoração e Gerenciamento de Eventos (MGE), prevista no ITIL 4, assume papel central ao definir diretrizes para detectar, registrar, correlacionar, classificar e tratar mudanças de estado relevantes nos serviços e componentes de TI [14]. Apesar de sua relevância operacional, ainda são escassas as investigações que contemplem, de forma integrada, todo o ciclo que vai da detecção automatizada à abertura e ao encerramento de *tickets* no contexto da administração pública municipal [15].

A literatura tem se concentrado predominantemente em processos de gerenciamento de incidentes e mudanças, enquanto a prática de Monitoração e Gerenciamento de Eventos permanece relativamente pouco explorada, sobretudo no contexto municipal, especialmente no que se refere à integração “ponta a ponta” entre monitoração, classificação adaptativa de criticidade e automação do tratamento [22], [21].

Diante desse contexto, este trabalho propõe uma arquitetura aberta e integrada, composta por ferramentas *open-source*, com o objetivo de automatizar o fluxo de MGE em uma instituição pública municipal. A proposta integra o Zabbix, responsável pela monitoração e detecção de eventos, um Motor de Inferência Fuzzy (MIF) desenvolvido em Python, voltado à classificação adaptativa de criticidade, e o GLPI, empregado para o gerenciamento do ciclo de vida dos *tickets*.

Ao combinar monitoração contínua, inferência Fuzzy multicritério e automação do tratamento, a arquitetura proposta busca reduzir tempos de resposta, eliminar etapas manuais, ampliar a rastreabilidade e aumentar a confiabilidade operacional dos serviços públicos digitais. Dessa forma, o modelo pretende responder a uma lacuna ainda presente na literatura e, simultaneamente, enfrentar uma demanda prática concreta observada no contexto institucional investigado.

A proposta também se justifica pelo potencial de replicabilidade em outros contextos da administração pública, especialmente em organizações que necessitam fortalecer seus mecanismos de governança de TIC sem depender de plataformas proprietárias de alto custo. Nesse sentido, o modelo busca conciliar aderência às boas práticas da ITIL 4 com viabilidade técnica e econômica para ambientes públicos de média e grande complexidade.

O estudo de caso concentra-se na Prefeitura Municipal de Arapongas-Pr, cuja área de Tecnologia da Informação gerencia uma infraestrutura extensa, heterogênea e composta por ativos críticos que conectam secretarias, prédios públicos e serviços essenciais. Essa amplitude e diversidade operacional configuram um cenário particularmente favorável à aplicação e avaliação do modelo GAIA-MGE proposto.

Além da relevância prática do ambiente selecionado, o recorte empírico oferece condições adequadas para examinar como uma arquitetura automatizada de MGE pode contribuir para padronização processual, melhoria da capacidade de resposta e fortalecimento da governança institucional. Assim, o estudo articula um problema concreto de operação de TI com uma proposta metodologicamente fundamentada e potencialmente transferível para outras administrações públicas.

A questão de pesquisa que orienta este estudo é a seguinte: *"como automatizar o fluxo de MGE, conforme as práticas da ITIL 4, integrando detecção, classificação adaptativa de criticidade e gestão de tickets em órgãos públicos municipais, de modo a otimizar a detecção, a análise e a resolução de incidentes, elevar a qualidade dos serviços de TIC e gerar valor público?"*

A partir dessa questão, a pesquisa busca contribuir para o avanço da governança e da gestão de serviços de TIC no setor público, ao propor um modelo que articula modelagem de processos, automação operacional e suporte à decisão em um fluxo integrado de MGE. Com isso, pretende-se oferecer tanto uma contribuição aplicada, voltada à resolução de um problema institucional concreto, quanto uma contribuição acadêmica, ao enfrentar uma lacuna identificada na literatura.

Este trabalho está organizado da seguinte forma: o Capítulo 1 apresenta a introdução ao tema, bem como os objetivos e a justificativa da pesquisa; o Capítulo 2 expõe a fundamentação teórica; o Capítulo 3 discute os trabalhos relacionados; o Capítulo 4 descreve a metodologia adotada; o Capítulo 5 detalha o modelo proposto, incluindo os fluxos operacionais, a avaliação de maturidade institucional e a arquitetura integrada do sistema; o Capítulo 6 apresenta a discussão dos resultados; o Capítulo 7 trata das limitações e dos trabalhos futuros; o Capítulo 8 traz a conclusão; o Capítulo 9 apresenta as contribuições da pesquisa; o Capítulo 10 aborda a disponibilidade de dados e artefatos; e o Capítulo 11 contempla as considerações de ética, seguidos das referências, apêndices e trabalhos publicados pelo autor.

1.1 Objetivo Geral

Esta pesquisa tem como objetivo conceber, implementar e validar, em caráter piloto, uma arquitetura de MGE alinhada à ITIL 4, capaz de automatizar o ciclo de detecção, classificação adaptativa de criticidade e abertura/fechamento de *tickets*, em uma instituição pública municipal.

A arquitetura é fundamentada em um fluxo de processos modelado em BPMN, que operacionaliza as etapas de monitoração, correlação, avaliação e tratamento de eventos, constituindo o eixo central do modelo proposto.

A proposta busca responder à ausência de modelos institucionais que integrem, de forma automatizada, a detecção de eventos, a classificação adaptativa de criticidade e o acionamento de fluxos de tratamento, lacuna que ainda compromete a eficiência e a padronização das respostas operacionais nos órgãos públicos.

A validação foi realizada em ambiente de testes segregado, alimentado em tempo real por registros provenientes da infraestrutura de um prédio público com alta demanda por serviços digitais e rigorosos requisitos de continuidade operacional, o que proporcionou um cenário adequado para a avaliação da proposta.

Espera-se que a arquitetura proposta contribua como referencial metodológico, fortaleça a governança de TIC e agregue valor público ao promover maior confiabilidade e transparência nos serviços digitais.

1.2 Objetivos Específicos

Para alcançar o objetivo geral proposto, esta pesquisa busca:

- Desenvolver um modelo conceitual de MGE fundamentado na ITIL 4, representado por um fluxo de processos em BPMN que sistematize as etapas de detecção, correlação, classificação e tratamento de eventos;
- Avaliar o nível de maturidade institucional em governança de TIC no período pré-implantação, utilizando a ferramenta GAIA, de modo a estabelecer o diagnóstico inicial do ambiente organizacional;
- Implementar uma arquitetura integrada, baseada em ferramentas *open-source*, Zabbix (monitoração), Motor de Inferência Fuzzy em Python (classificação adaptativa de criticidade) e GLPI (gestão de *tickets*), capaz de automatizar o ciclo de vida de eventos e chamados;
- Validar o modelo em ambiente piloto em um órgão público de alta demanda, analisando sua viabilidade técnica, desempenho e aderência às práticas de governança de TIC;
- Estabelecer a linha de base quantitativa do cenário pré-implantação, por meio da análise dos indicadores *Mean Time to Detect* (MTTD) e *Mean Time to Repair* (MTTR) do sistema legado, bem como discutir, com base na execução piloto, o potencial de melhoria operacional e de evolução da maturidade institucional com a adoção do modelo proposto.

1.3 Justificativa

A transformação digital nos municípios brasileiros intensificou a dependência de serviços eletrônicos para a oferta de políticas públicas, ao mesmo tempo em que elevou a complexidade operacional das infraestruturas de Tecnologia da Informação e Comunicação (TIC) [7].

A literatura especializada revela uma lacuna específica no ciclo de MGE, faltam modelos que integrem, de forma automatizada, a detecção de anomalias, a classificação adaptativa de criticidade e a abertura/fechamento de *tickets* no contexto municipal [15], [22].

A ausência dessa integração eleva o MTTD e o MTTR, gerando respostas reativas pouco padronizadas, um quadro ainda mais crítico em municípios de médio porte, onde as equipes são enxutas e os recursos orçamentários limitados. Avaliações prévias indicam maturidade institucional “baixa” em governança de TIC nos governos locais brasileiros, destacando a urgência de soluções metodológicas replicáveis [23], [24].

O modelo proposto neste trabalho, surge exatamente como resposta a esse cenário, ao estruturar um fluxo automatizado de MGE capaz de consolidar processos, dados e decisões de forma integrada.

Abordagens híbridas que combinam LF, processamento de linguagem natural e aprendizado por reforço demonstram ganhos concretos na priorização dinâmica de incidentes, ao lidar com a vaguidade linguística das descrições textuais e adaptar-se ao comportamento operacional em tempo real [25]. Esses resultados sugerem que a incorporação de raciocínio Fuzzy interpretável a um *framework* ITIL 4 pode elevar tanto a precisão de classificação quanto a transparência exigida no setor público.

Nesse contexto, justifica-se o desenvolvimento de uma arquitetura aberta e integrada de MGE, alinhada à ITIL 4 e sustentada por ferramentas *open-source*, voltada à redução do esforço manual nas atividades de monitoração e resposta, à padronização do fluxo de eventos segundo boas práticas internacionalmente reconhecidas e ao fortalecimento da maturidade de governança de TIC em ambientes municipais.

Além de sua contribuição técnica, a pesquisa possui relevância social ao fortalecer a capacidade das prefeituras em garantir a continuidade e a confiabilidade dos serviços públicos digitais, aspectos essenciais para a efetividade das políticas públicas e para a confiança do cidadão no governo eletrônico.

O aprimoramento da governança de TIC contribui diretamente para a eficiência administrativa, a transparência e a sustentabilidade das ações governamentais, ampliando o impacto positivo da transformação digital na esfera pública [26].

A pesquisa responde, assim, a uma demanda prática concreta e a uma lacuna teórica identificada na literatura, ao propor um modelo replicável que pode orientar outras administrações públicas na adoção de rotinas de MGE mais eficazes, padronizadas, ágeis e orientadas à geração de valor público.

2. FUNDAMENTAÇÃO TEÓRICA

Esta seção apresenta os conceitos, métodos e referências que sustentam este trabalho, destacando abordagens consolidadas e soluções para gestão automatizada de monitoração e gerenciamentos de eventos de TIC.

2.1. Governança e Gerenciamento de Serviços de TI: ITIL 4 e COBIT 2019

O ITIL 4 consolida boas práticas que integram pessoas, processos e tecnologias para elevar eficiência, qualidade e valor gerado pelos serviços de TI [1]. Entre as 34 práticas descritas, o Gerenciamento de Eventos é essencial para detectar, analisar e responder a ocorrências capazes de comprometer disponibilidade ou desempenho. Quando automatizada, essa prática reduz intervenção manual e acelera o tempo de resposta, beneficiando organizações de diferentes portes [14], [24], [27], [28].

Em complemento ao ITIL, o COBIT 2019 também se destaca como *framework* de governança de TI amplamente adotada em organizações públicas e privadas, fornecendo diretrizes de alto nível para controle, ‘auditoria e alinhamento estratégico dos processos de TI [18]. Embora COBIT e ITIL possam ser aplicados de forma conjunta e complementar, este trabalho adota o ITIL 4 por seu foco operacional e suas práticas detalhadas para automação do Gerenciamento de Eventos, enquanto o COBIT serve como referência para estruturação da governança em níveis mais abrangentes.

2.2. A Prática de Monitoramento e Gerenciamento de Eventos (MGE) em Instituições Públicas

A prática MGE no ITIL 4 compreende as etapas de (*i*) detectar mudanças de estado nos serviços/componentes; (*ii*) registrar os eventos, (*iii*) classificar (informativo, alerta ou exceção); (*iv*) priorizar com base em impacto e urgência; e (*v*) responder (iniciando ações como notificações, automação ou escalonamento para incidentes ou problemas. Essa observação contínua visa evitar falhas e melhorar a disponibilidade de serviços de TIC [1].

Essa sequência de atividades constitui o núcleo funcional da prática de Monitoração e Gerenciamento de Eventos (MGE), cuja finalidade é assegurar a observação

contínua do ambiente de tecnologia da informação e a pronta identificação de alterações que possam comprometer a estabilidade operacional.

Conforme o ITIL 4, a efetividade dessa prática depende da definição de parâmetros de monitoração, correlação e limiares de alerta, bem como da aplicação de procedimentos sistematizados de priorização e resposta.

Desse modo, a MGE estabelece uma integração direta entre a monitoração proativa e o gerenciamento reativo de incidentes, favorecendo a antecipação de falhas e a manutenção dos níveis de desempenho, disponibilidade e continuidade dos serviços de TIC.

No contexto brasileiro, o Mapa de Governo Digital 2022 [11], a demanda por serviços digitais aumentou em 94% das prefeituras brasileiras desde a pandemia de Covid-19, mas 18% dessas cidades ainda classificam a integração de sistemas e a abertura de dados como “ruim” ou “muito ruim” [11].

Situação semelhante foi constatada em instituições públicas de ensino da Lituânia, sem um processo unificado de MGE, essas organizações apresentavam baixa rastreabilidade de incidentes e respostas reativas; a adoção completa do ITIL 4 elevou a visibilidade operacional e encurtou prazos de resolução [29].

Segundo [30], analisaram tendências e desafios em governança de segurança da informação no setor público e destacaram que a maioria dos municípios ainda opera com processos de monitoramento fragmentados, sem integração ponta-a-ponta e sem automação completa no fluxo de eventos e incidentes. Os autores ressaltam que a falta de processos integrados compromete a rastreabilidade, a agilidade e a confiabilidade operacional nos governos locais.

Para [15], os autores observam que, apesar dos avanços tecnológicos, grande parte das abordagens para monitoramento e gerenciamento de alertas e incidentes em órgãos públicos ainda se caracteriza por soluções isoladas, limitando a eficiência do tratamento automático e a integração dos processos de detecção, classificação e resposta.

2.3. Modelagem de Processos com BPMN

A *Business Process Model and Notation* (BPMN 2.0) consolidou-se como padrão internacional para modelagem de processos, permitindo representar fluxos de forma compreensível para equipes técnicas e administrativas [31].

Na Administração Pública, seu uso tem se mostrado eficaz para padronizar procedimentos, reduzir ambiguidades e apoiar iniciativas de automação, conforme demonstram estudos aplicados em instituições públicas que evidenciam ganhos de rastreabilidade, clareza e coordenação operacional [32], [33], [34].

Esses resultados reforçam a adequação da BPMN como linguagem de documentação de processos, uma vez que permite representar decisões, exceções, papéis e interações de forma sistemática e auditável [35].

No contexto deste trabalho, tais características são essenciais para modelar o fluxo de MGE alinhado ao ITIL 4, pois possibilitam explicitar regras decisórias, pontos de controle e caminhos alternativos do processo.

A partir dessas evidências, a modelagem em BPMN torna-se o alicerce para representar, estruturar e operacionalizar o fluxo de Monitoração e Gerenciamento de Eventos adotado neste trabalho, permitindo que o modelo proposto traduza requisitos técnicos e regras decisórias em um processo padronizado, auditável e alinhado às práticas do ITIL 4.

2.4. Avaliação de Maturidade em Governança de TIC

A avaliação de maturidade constitui a base conceitual que orienta pesquisas sobre governança de TIC, pois traduz observações qualitativas em métricas objetivas e comparáveis.

De forma geral, os modelos de maturidade descrevem estágios evolutivos que vão do nível inicial ao otimizado, avaliando dimensões como processos, pessoas, tecnologia e resultados. Essa abordagem permite identificar o grau de institucionalização das práticas, priorizar investimentos e monitorar a evolução ao longo do tempo [36].

Estudos subsequentes, propõem ajustes para tornar essas escalas mais aderentes à realidade do setor público. [37] defendem a inclusão de variáveis orçamentárias e de metas ligadas ao valor público gerado pelos serviços de TIC, argumentando que esses fatores afetam diretamente a capacidade de avanço entre os níveis de maturidade.

Por sua vez, [38] destaca a necessidade de incorporar critérios de risco e de conformidade regulatória, enfatizando que a maturidade só se eleva de forma sustentável quando a TI entrega benefícios claros à sociedade e obedece às normas vigentes.

Estudos empíricos indicam ganhos concretos quando se aplica a avaliação de maturidade, organizações públicas que adotaram modelos estruturados conseguiram redefinir prioridades de investimento, reduzir redundâncias operacionais e estabelecer metas de evolução realistas, demonstrando transparência perante órgãos de controle [37].

Assim, mensurar a maturidade da governança de TI não é apenas exercício teórico, mas um mecanismo essencial para planejar recursos, mitigar riscos e comprovar a geração de valor público.

2.5. Inferência de Criticidade por Lógica Nebulosa (Fuzzy)

A Lógica Nebulosa ou *Fuzzy Logic* (FL), proposta por [2], introduz o conceito de "verdade parcial", permitindo que valores pertençam a um conjunto em diferentes graus de pertinência. Esse grau é um número real no intervalo (0 e 1), sendo o valor = 0 indica ausência total de pertencimento e o valor = 1, pertencimento completo, valores intermediários representam níveis parciais. Essa flexibilidade supera o binômio (verdadeiro/falso) da lógica booleana tradicional e viabiliza a modelagem de ambiguidades típicas de fenômenos do mundo real.

Um sistema de inferência Fuzzy organiza-se em quatro etapas fundamentais: (*i*) fuzzificação, (*ii*) conjunto de regras, (*iii*) inferência e (*iv*) defuzzificação.

Na primeira etapa, a fuzzificação, cada variável de entrada originalmente nítida "*crisp*" (um valor numérico exato que chega ao sistema sem ambiguidade) como impacto e urgência medidos em valores absolutos é convertida em graus de pertinência que variam de 0 a 1. Esse mapeamento é feito por funções de pertinência cujos formatos determinam como a transição entre categorias ocorre; ao transformar números exatos em representações graduais, a etapa de fuzzificação cria a base para que o sistema trate incertezas de forma quantitativa [3], [4].

A seguir vem o conjunto de regras. Sentenças do tipo se impacto é alto e urgência é média então criticidade é elevada encapsulam conhecimento especialista em linguagem próxima do natural, facilitando validação com operadores de rede [3].

A inferência aplica essas regras segundo o esquema Mamdani, introduzido por [39]. Nesse formato, tanto as premissas quanto as conclusões permanecem Fuzzy, ou seja, (representadas por conjuntos com graus de pertinência e fronteiras imprecisas), o que simplifica a modelagem heurística (baseada em regras práticas e aproximações empíricas) e torna o raciocínio do sistema transparente.

Durante a agregação, todos os conjuntos gerados pelas regras ativadas são combinados em uma única superfície nebulosa. Essa união preserva as contribuições individuais e evita a perda de informações potencialmente conflitantes, fornecendo um panorama contínuo das recomendações de criticidade [4].

A defuzzificação converte a superfície agregada em um valor numérico único. O método do centroide, adotado aqui, calcula o "centro de gravidade" da área resultante, mantendo nuances entre níveis adjacentes e evitando saltos abruptos quando as entradas variam pouco [3].

Quanto às funções de pertinência, a lógica Fuzzy (LF) admite perfis triangulares, trapezoidais e em sino (*bell-shaped*). Opta-se pelas curvas em sino porque elas suavizam ainda mais as transições, reduzem a sensibilidade a ruído nas medições de impacto e urgência e elevam a estabilidade das classificações, benefício já observado em aplicações de priorização de incidentes e análise de risco [40], [41].

2.6. A Matriz Multicritério

A priorização de eventos e incidentes em TI normalmente combina múltiplos critérios, sobretudo impacto e urgência, conforme o ITIL 4 [1]. A forma mais comum é a matriz 5x5: cada eixo recebe níveis de 1 a 5 e o cruzamento das 25 células é mapeado para prioridades (P1 a P5) por uma tabela.

Esse modelo é simples e operacional, mas usa limiares fixos; por isso, casos de fronteira (na transição entre categorias) podem sofrer saltos de prioridade com pequenas variações (por exemplo, impacto de 3 para 4 mudando de P3 para P4), o que reduz a sensibilidade em contextos incertos ou com medições ruidosas [40], [41].

A literatura recente tem explorado a aplicação de métodos multicritério aliados à LF para refinar a matriz de priorização, permitindo transições mais suaves entre os níveis e maior aderência ao contexto real da operação [42], [41].

Ao atribuir graus de pertinência às variáveis de entrada, o modelo de LF multicritério oferece decisões mais adaptativas e robustas, superando limitações inerentes aos modelos puramente categóricos.

Essa abordagem se fundamenta em princípios consolidados de decisão multicritério [43], permitindo não apenas a integração de conhecimento especializado, mas também o alinhamento com as melhores práticas internacionais de gestão de incidentes.

Assim, a matriz multicritério baseada em LF viabiliza uma priorização contínua e sensível ao contexto, contribuindo para maior eficiência operacional e melhor qualidade do serviço prestado.

2.7. Service Desk e GLPI como ITSM Open Source

O GLPI é uma suíte *open source* de Gerenciamento de Serviços de TI, ou *Information Technology Service Management* (ITSM), que reúne catálogo de serviços, registro de incidentes, Base de Dados de Gerenciamento de Configuração, ou *Configuration Management Database* (CMDB), gestão de contratos e relatórios de Acordos de Nível de Serviço, ou *Service Level Agreement* (SLA), sustentada por arquitetura modular *PHP/MySQL* e *API REST* com autenticação por *token* e *webhooks*, o que facilita integrações com ferramentas de monitoração e automação [44].

Soluções *open source* de ITSM despontam como alternativas viáveis às suítes proprietárias, sobretudo quando a organização busca reduzir custos de licenciamento sem comprometer governança. Uma revisão sistemática recente identificou o GLPI (junto a iTop[1] e OTRS[2]) como o software livre mais recorrente para orquestrar o ciclo de vida de incidentes, manter a CMDB e controlar SLAs, evidenciando ganhos de rastreabilidade e aderência às melhores práticas [45].

Estudos empíricos pós 2022, exploram diretamente a base de dados do GLPI. Segundo [46], analisaram mil chamados reais de um órgão público, aplicando técnicas de classificação de *tickets* para otimizar o fluxo de atendimento e mostrando que a suíte fornece atributos estruturados suficientes para experimentos de automação.

Para [47], os autores investigaram o uso de metodologias ágeis em ITSM com o GLPI exposto via *API REST*, validando automatizações de backlog e priorização. Quando centraliza o ciclo de vida dos *tickets* e integra-se a ferramentas de monitoramento, o GLPI assume o papel de fonte única de verdade dentro de uma arquitetura orientada a serviços.

2.8. Idempotência e Deduplicação de Incidentes

A idempotência é introduzido por [48]como atributo de métodos *HTTP* no desenho de arquiteturas *REST*, operações *GET, PUT e DELETE* devem produzir o mesmo

[1] Disponível em: https://www.itophub.io/
[2] Disponível em: https://otrs.com/

estado mesmo que sejam repetidas, assegurando confiabilidade diante de retransmissões inevitáveis em sistemas distribuídos. [49] amplia o conceito para o domínio corporativo ao propor o padrão Operação Idempotente (*Idempotent Operation*) em *scripts* transacionais, recomendando que comandos críticos armazenem uma chave única para reconhecer reexecuções e, assim, prevenir efeitos colaterais em ambientes de alto volume.

De acordo com [50], o autor adapta esses princípios a ecossistemas de *microservices* e APIs (Interface de Programação de Aplicações) modernas, cada requisição carrega um *token* idempotente (ID) que o consumidor utiliza para descartar duplicatas, garantindo execuções *at-least-once* (pelo menos uma vez) sem gerar múltiplos registros.

No fluxo Zabbix, MIF e GLPI, essa estratégia permite que o serviço de monitoração reenvie *webhooks* sem risco de abrir *tickets* em duplicidade, fortalecendo a robustez da automação de incidentes.

2.9. Métricas de Desempenho Operacional: MTTD e MTTR

O sistema de gestão de serviços de TI deve medir, analisar e avaliar continuamente o seu desempenho, conforme exige [51], que integra o ciclo de melhoria contínua do *Service Management System* (SMS).

Entre os indicadores recomendados, destacam-se o MTTD e o MTTR, amplamente utilizados em pesquisas recentes sobre observabilidade e resposta a incidentes em ambientes distribuídos[52].

Além do respaldo normativo, estudos recentes reforçam a centralidade das métricas MTTD e MTTR na modernização dos processos de monitoramento e resposta a incidentes.

Segundo [53], demonstram que a adoção de modelos de monitoramento em tempo real integrando coleta avançada de dados, alertas automatizados e dashboards dinâmicos, permite significativa redução dos tempos médios de detecção e resolução, viabilizando respostas mais ágeis e proativas em ambientes complexos de TI. A literatura evidencia que tais métricas, quando incorporadas à estratégia operacional, contribuem para elevar a resiliência, reduzir indisponibilidades e orientar ciclos de melhoria contínua nos sistemas de gestão de serviços.

Estudos recentes corroboram a relevância das métricas MTTD e MTTR para a efetividade dos sistemas de gestão de incidentes de segurança da informação. Conforme [54] destacam que a mensuração dessas métricas constitui um dos principais indicadores de

desempenho operacional em gerenciamento de incidentes, sendo fundamentais para avaliar a capacidade de resposta, eficiência operacional e resiliência organizacional diante de ameaças.

Os autores ressaltam que a redução dos tempos médios de detecção e resposta está diretamente relacionada à adoção de soluções modernas de monitoramento, automação e inteligência artificial, em conformidade com padrões internacionais. A análise sistemática desses indicadores, integrada a *frameworks* de segurança e processos de melhoria contínua, viabiliza não apenas respostas mais rápidas, mas também o aprimoramento constante das estratégias de defesa cibernética.

3. TRABALHOS RELACIONADOS

A literatura recente em gestão de incidentes e monitoração de serviços de TIC apresenta avanços significativos em diferentes frentes, desde a modelagem formal de processos até técnicas inteligentes de detecção e priorização de eventos.

Estudos como os de Alonso (2020) [33], Aguilar (2023) [55] e Tavantzis (2023) [34], evidenciam maturidade crescente no uso de BPMN e estruturas decisórias para representar fluxos operacionais de forma clara e auditável.

No campo da monitoração, pesquisas como Nguyen (2024) [56], Tao (2025) [57] e Klots (2025) [58], demonstram progressos relevantes na aplicação de inteligência artificial, arquiteturas distribuídas e detecção de anomalias aplicadas a ambientes complexos.

Paralelamente, trabalhos que empregam LF e métodos multicritério, a exemplo de Peralta (2025) [59], Tomak e Polat (2022) [40] e Mrówczyńska (2022) [60], avançam na priorização e classificação de eventos sob incerteza, ainda que permaneçam focadas em componentes isolados do ecossistema de gestão.

Diante dessa diversidade, torna-se necessário organizar a literatura em eixos que permitam compreender convergências, limites e interdependências. Assim, esta seção estrutura os estudos em cinco domínios principais: (*i*) modelagem de processos; (*ii*) monitoração e detecção de eventos; (*iii*) priorização baseada em lógica Fuzzy e métodos multicritério; (*iv*) automação do ciclo de vida de *tickets*, incluindo deduplicação e integração com plataformas ITSM; e (*v*) referenciais de governança, maturidade e boas práticas aplicados à gestão de serviços de TIC.

Essa classificação evidencia contribuições relevantes, mas também demonstra que grande parte das pesquisas permanece restrita a fragmentos do problema, sem integração operacional ponta-a-ponta.

A produção científica sobre gestão de incidentes e monitoração distribui-se em diferentes frentes conceituais e tecnológicas, o que exige uma organização temática para orientar a análise. Assim, os estudos são agrupados em eixos que refletem seus focos principais, permitindo situar suas contribuições no panorama atual e preparar a discussão detalhada apresentada a seguir.

3.1. Modelagem de Processos

Alonso (2020) [33], modela o processo de gerenciamento de incidentes em uma instituição pública utilizando BPMN, demonstrando que a representação formal do fluxo reduz ambiguidades e melhora a coordenação operacional. Seu estudo evidencia o papel da modelagem como mecanismo de padronização e controle.

Pereira (2020) [61], redesenha processos de atendimento de incidentes por meio de BPMN, enfatizando como a documentação clara das atividades possibilita identificação de redundâncias e aprimora o desempenho operacional. A abordagem destaca a modelagem como ferramenta central para análise de processos.

Aguilar (2023) [55], combina BPMN com matriz RACI para estruturar atividades de resposta a incidentes críticos, buscando explicitar papéis e responsabilidades no fluxo. O estudo reforça a importância de governança processual em ambientes de alta criticidade.

Dzemydiene (2023) [29], discute a adoção das práticas do ITIL 4 em instituições públicas, analisando como frameworks consolidados contribuem para padronização e integração de serviços. O trabalho evidencia limitações e benefícios de modelos de governança aplicados à infraestrutura de TI.

Tavantzis (2023) [34], integra BPMN e *Decision Model and Notation* (DMN) para modelar processos que dependem de decisões estruturadas, demonstrando como a formalização das regras decisórias aumenta rastreabilidade e consistência operacional. O estudo destaca a sinergia entre fluxo e lógica de decisão.

Ashmoery (2024) [17], analisa a convergência entre *Lean Management* (Lean), Agile, *Development Operations* (DevOps) e ITIL 4 na modernização do ITSM, discutindo ganhos de eficiência e redução de desperdícios. O autor mostra como abordagens híbridas podem fortalecer a governança e a agilidade operacional.

Teixeira (2024) [62], utiliza Business Process Management (BPM) para investigar e reestruturar processos organizacionais, identificando gargalos e oportunidades de melhoria. O estudo reforça o papel do BPM como instrumento de racionalização da operação.

Licardo (2024) [63], propõe um método automatizado para gerar modelos BPMN a partir de textos, visando reduzir esforço manual e aumentar consistência na documentação de processos. A abordagem contribui para a padronização das representações organizacionais.

Mariya (2024) [64], discute o uso da BPMN como ferramenta de colaboração e comunicação entre equipes, mostrando que representações visuais favorecem compreensão compartilhada e melhoria da coordenação operacional.

3.2. Monitoração e Detecção de Eventos

Johnson (2024) [53], desenvolve modelos de monitoramento contínuo para reduzir MTTR, destacando a importância da visibilidade em tempo real para resposta rápida a incidentes. O estudo evidencia o papel de métricas e monitoramento na melhoria da gestão de operações.

Nguyen (2024) [56], aplica *Artificial Intelligence for IT Operations* (AIOps) à análise de fluxos de eventos, propondo mecanismos inteligentes de detecção automática de anomalias. O estudo demonstra que a automação baseada em aprendizado melhora eficiência e reduz alertas irrelevantes.

Tao (2025) [57], desenvolve um método distribuído para detecção de anomalias em redes de grande escala, abordando requisitos de desempenho e escalabilidade. O trabalho reforça a importância de arquiteturas distribuídas para suporte à monitoração intensiva.

Reis (2020) [65], descreve a implantação prática do Zabbix em ambiente universitário, destacando benefícios operacionais como centralização do monitoramento, melhoria na disponibilidade e padronização de métricas.

Vázquez et al. (2020) [66], apresentam uma arquitetura de monitoramento *open-source* integrada a sensores da *Internet of Things* (IoT) para ampliar a observabilidade de infraestruturas de TI. O estudo demonstra que a combinação entre coleta distribuída de dados e um servidor Zabbix centralizado melhora a visibilidade operacional e reduz custos, evidenciando o potencial de soluções modulares para monitoramento em ambientes de grande porte.

Matte (2020) [67], compara ferramentas de monitoramento de redes, analisando atributos técnicos, desempenho e aplicabilidade. O estudo fornece critérios para seleção de sistemas *Network Management System* (NMS) conforme cenários e exigências específicas.

Guo (2024) [68], apresenta o uso do Zabbix em redes de campus inteligente, valorizando arquitetura distribuída e escalabilidade. O estudo demonstra como soluções de monitoramento podem suportar ambientes heterogêneos e de grande porte.

Rodrigues (2024) [69], avalia o impacto do Zabbix em ambientes hospitalares, mostrando como o monitoramento estruturado melhora segurança, disponibilidade e eficiência. O estudo destaca a relevância de *Network Management System* (NMS) em operações críticas.

Klots (2025) [58], integra o Zabbix com algoritmos de aprendizado de máquina para detecção preditiva de anomalias, indicando que a combinação entre monitoramento e Inteligência Artificial (IA) reduz falhas e melhora previsibilidade.

3.3. Fuzzy / Multicritério

Leite (2024) [70], utiliza lógica Fuzzy para apoiar decisões operacionais sob incerteza, demonstrando como variáveis linguísticas permitem avaliações mais flexíveis. O estudo reforça a utilidade de sistemas Fuzzy na modelagem qualitativa de fenômenos complexos.

Peralta (2025) [25], em seu estudo baseado em aprendizagem por reforço, integra lógica Fuzzy com algoritmos adaptativos para priorização de incidentes, propondo um modelo que ajusta decisões conforme aprendizado contínuo.

Peralta (2025) [59], em seu trabalho de *Natural Language Processing* (NLP), aplica inferência Fuzzy a descrições textuais de incidentes, convertendo linguagem natural em classificações estruturadas. O estudo mostra como técnicas linguísticas podem apoiar priorização automática.

Olano Garcés (2025) [41] propõe um modelo de priorização de incidentes unindo ITIL e lógica Fuzzy, demonstrando resultados aplicados no setor de TI de universidades. O estudo reforça o uso de regras linguísticas para classificação de severidade.

Oliveira (2025) [71], investiga a combinação de inteligência artificial e lógica Fuzzy em processos industriais, apresentando mecanismos híbridos de inferência para tomadas de decisão sob múltiplas variáveis.

Fujita (2025) [72], desenvolve fundamentos matemáticos avançados para sistemas Fuzzy e neutrosóficos, ampliando capacidade expressiva e precisão de modelos de inferência. Seu trabalho aprofunda teorias utilizadas em abordagens multicritério.

Ranggadara (2019) [73], integra ITIL e lógica Fuzzy para aprimorar priorização de incidentes, propondo regras linguísticas para lidar com fatores subjetivos. O estudo destaca que Fuzzy torna avaliações mais consistentes.

Slavyanov (2024) [74], utiliza lógica Fuzzy em análises pós-incidente, oferecendo metodologia para avaliar impacto e risco a partir de variáveis qualitativas. O estudo contribui para entendimento retrospectivo do comportamento de incidentes.

Mrówczyńska (2022) [60], apresenta um método multicritério baseado em Fuzzy sets para avaliação de riscos, estruturando uma abordagem robusta para classificação em ambientes de incerteza e múltiplas dimensões.

Funika (2015) [75], compara automação de monitoramento baseada em regras e em lógica Fuzzy, demonstrando vantagens da abordagem Fuzzy para cenários dinâmicos. O estudo reforça adaptabilidade como atributo essencial.

Alfarhan (2018) [76], propõe um modelo de avaliação de serviços de TI utilizando números Fuzzy triangulares, buscando representar subjetividade e variações de percepção na análise de qualidade.

Tomak e Polat (2022) [40], desenvolvem um modelo multicritério para priorizar riscos, combinando fatores críticos de sucesso com técnicas estruturadas de decisão. O estudo contribui para métodos de avaliação em cenários complexos.

Gu (2024) [77], em seu trabalho sobre *Soft Prototype-based Autonomous Fuzzy Inference System* (SPAFIS), apresenta um sistema de detecção de intrusões baseado em inferência Fuzzy autônoma, projetado para redes de grande escala. O estudo destaca precisão e adaptabilidade na identificação de ameaças.

Abdullah (2018) [78], propõe um mecanismo Fuzzy evolutivo para análise temporal de eventos, utilizando séries históricas para aprimorar a classificação adaptativa. O estudo reforça o uso de Fuzzy como estratégia para tratar variações e incertezas no monitoramento.

3.4. Automação / GLPI - *Tickets*

Vasconcellos (2017) [79], compara diferentes plataformas ITSM, como GLPI, OTRS, RT e OCOMON, avaliando funcionalidades, limitações e características operacionais. Seu estudo oferece base para seleção de ferramentas de suporte.

Liu et. al. (2023) [80], apresenta um método para detectar e agrupar *tickets* duplicados em sistemas cloud, utilizando técnicas estatísticas para reduzir redundância e melhorar eficiência do atendimento.

Chen et. al. (2021) [81], propõem uma abordagem baseada em grafos para identificar relacionamentos entre *tickets*, possibilitando detecção de duplicidade e agregação de registros correlatos em ambientes de TI.

Achmad et. al. (2023) [82], aplica redes *Long Short-Term Memory* (LSTM) para prever abertura de *tickets* no GLPI, propondo um modelo preditivo que antecipa demandas e melhora planejamento do suporte técnico.

3.5. Governança / Maturidade / ITIL

Karatas (2023) [19], realiza uma revisão sistemática sobre mecanismos de governança de TI, sintetizando principais práticas, modelos e desafios enfrentados por organizações na adoção de estruturas formais de controle.

Magnusson (2025) [30], investiga a governança de segurança no setor público, analisando diretrizes, políticas institucionais e barreiras operacionais. O estudo destaca a complexidade da gestão de segurança em ambientes governamentais.

Serrano (2020) [83], analisa práticas de gestão de infraestrutura com base no ITIL, identificando lacunas e oportunidades de melhoria em processos operacionais. O estudo argumenta pela importância de padronização e governança.

Yandry (2019) [84], propõe um modelo de maturidade ITSM baseado em lógica Fuzzy, permitindo avaliações mais flexíveis da capacidade organizacional ao lidar com dimensões qualitativas e incertezas.

Neto (2020) [38], examina governança pública de TI em administrações municipais, identificando fragilidades estruturais e desafios na gestão estratégica. O estudo discute limites institucionais que afetam a adoção de boas práticas.

Santos (2020) [37], propõe um modelo de maturidade em TIC estruturado em múltiplas dimensões e níveis evolutivos, oferecendo critérios para avaliação institucional e evolução de capacidades organizacionais.

Ueno (2018) [85], apresenta o modelo de maturidade GAIA para avaliar a capacidade institucional necessária à implantação da continuidade de serviços de TI. O estudo estrutura dimensões organizacionais relacionadas à governança, processos e competências, oferecendo um instrumento sistemático para diagnóstico e evolução da maturidade.

A análise comparativa dos 43 estudos evidencia que, embora diversas contribuições avancem simultaneamente em mais de um eixo, como modelagem de processos, monitoramento inteligente, técnicas de inferência Fuzzy ou mecanismos de governança a literatura permanece fragmentada no que diz respeito à integração plena desses componentes em um fluxo operacional coerente.

Mesmo quando abordam dois ou mais domínios, os trabalhos analisados não articulam essas dimensões de forma contínua e automatizada, deixando de configurar um ciclo completo de Monitoração e Gerenciamento de Eventos alinhado às práticas do ITIL 4.

Nesse contexto, o modelo proposto diferencia-se por apresentar uma arquitetura unificada capaz de automatizar integralmente o ciclo de MGE, articulando modelagem de processos, monitoração contínua, inferência Fuzzy multicritério, idempotência e integração com o sistema de *tickets*.

Para explicitar de maneira sistemática como essa abordagem supera a fragmentação observada na literatura, a Tabela 1, a seguir, sintetiza para cada estudo analisado, a lacuna correspondente, destacando os elementos não contemplados por cada autor e evidenciando a originalidade e abrangência da solução desenvolvida.

Tabela 1 - Resumo de Trabalhos Relacionados x Eixos x Lacuna

Eixo Temático	**Trabalhos (Autor/Ano)**	**Lacuna**
Modelagem de Processos (BPMN/DMN/BPM)	Alonso (2020); Pereira (2021); Aguilar (2023); Tavantzis (2023); Teixeira (2024); Licardo (2024); Mariya (2024).	Trabalhos concentram-se na modelagem estrutural, mas não integram monitoração operacional, classificação Fuzzy, idempotência ou automação de *tickets*, permanecendo em nível descritivo.
Monitoração e Detecção de Eventos (Zabbix, AIOps, Anomalias, IDS)	Johnson (2024); Nguyen (2024); Tao (2025); Zabbix UFAL (2020); Matte (2020); Guo – Campus (2024); Vázquez et al. (2020); Rodrigues (2024); Klots (2025).	Estudos tratam da detecção e análise de eventos, porém não conectam os resultados a processos BPMN, nem aplicam priorização Fuzzy ou automação integrada de *tickets* com garantia de idempotência.
Fuzzy e Métodos Multicritério (MFMC, NLP+Fuzzy, IDS Fuzzy)	Leite (2024); Peralta (2025–QL); Peralta (2025–NLP); Olano Garcés (2025); Oliveira (2025); Fujita (2025); Ranggadara (2019); Slavyanov (2024); Mrówczyńska (2022); Funika (2015); Alfarhan (2018); Alfarhan extra (2018); Tomak & Polat (2022); Yandry (2019); Pascarella (2021); Gu (2024 – SPAFIS); Abdullah (2018 – TiSEFE).	Avanços importantes em classificação Fuzzy e métodos multicritério, mas não há integração com NMS (Zabbix), nem com GLPI, muito menos um fluxo end-to-end que una BPMN, idempotência e automação de MGE.

Automação de *Tickets* / GLPI / Deduplicação	Vasconcellos (2017); Liu et. al. (2023); Chen et. al. (2021); Achmad et. al. (2023).	Trabalhos concentram-se na automação de *tickets*, mas não vinculam GLPI a eventos monitorados em tempo real, nem aplicam matriz Fuzzy multicritério ou lógica de idempotência acoplada ao processo.
Governança, ITIL e Maturidade Institucional	Dzemydiene (2023); Ashmoery (2024); Karatas (2023); Magnusson (2025); Serrano (2020); Neto (2020); Santos (2020).	Estudos fortalecem fundamentos de governança, mas não apresentam implementação técnica integrada, sem módulos de monitoramento, inferência Fuzzy ou automação operacional do MGE.

A análise desses eixos demonstra que, embora existam avanços importantes, a literatura ainda carece de modelos que combinem de forma coordenada monitoração contínua, inferência inteligente, processos formais e automação operacional.

Mesmo trabalhos mais abrangentes, como Ashmoery (2024) [17] e Dzemydiene (2023) [29], não alcançam arquiteturas que integrem BPMN, NMS, Fuzzy e orquestração automática de *tickets*.

Nesse contexto, o modelo proposto diferencia-se ao unificar ZABBIX, inferência Fuzzy multicritério, idempotência e automação no GLPI, oferecendo um ciclo completo de MGE alinhado ao ITIL 4 e superando a fragmentação identificada na literatura.

.

4. METODOLOGIA

Esta seção descreve a abordagem metodológica adotada, detalhando os procedimentos, técnicas e ferramentas utilizadas para a implementação de um sistema automatizado de monitoração e gerenciamento de eventos de TIC.

4.3. Metodologia de Pesquisa

Conforme destaca [86], a validade de estudos aplicados em ambiente organizacional é fortalecida quando se recorre a múltiplas fontes de evidência e a estratégias de triangulação sistemática.

Atendendo a esse princípio, a presente pesquisa, voltada à concepção e validação de um modelo de monitoramento e gerenciamento de eventos de TIC em uma instituição pública municipal, adota um método misto convergente, integrando técnicas qualitativas e procedimentos quantitativos.

Como instrumentos de coleta foram utilizados: um questionário em escala Likert aplicado via *Google Forms*, um instrumento de avaliação de avaliação de maturidade GAIA [87] e a coleta de indicadores quantitativos do sistema legado (MTTD, MTTR). Essa combinação, ao reunir dados narrativos e métricos de forma simultânea, amplia o alcance explicativo e a confiabilidade dos achados, conforme argumentam [88].

Do ponto de vista lógico-metodológico, o estudo apresenta caráter exploratório, por mapear práticas existentes e identificar lacunas no fluxo de monitoramento, além de orientação dedutiva, pois parte da prática de Monitoração e Gerenciamento de Eventos, (MGE) do ITIL 4 para formular hipóteses acerca da eficácia do artefato.

Essa articulação entre descrição inicial do fenômeno e teste de proposições derivadas de referenciais consolidados atende à recomendação de [89] para pesquisas que combinam fundamentação teórica rigorosa a análise empírica sistemática.

4.3.1. Abordagem Metodológica: Design Science Research (DSR)

A pesquisa adota a *Design Science Research* (DSR) como orientação metodológica para o desenvolvimento do artefato. Nesse contexto, utiliza-se a base conceitual de [5], que estrutura a DSR a partir de três ciclos complementares: (*i*) Relevância, que conecta

o estudo às necessidades e restrições do ambiente organizacional; (*ii*) Rigor, que assegura a utilização de fundamentos teóricos e métodos consolidados; e (*iii*) Design, responsável pela construção, revisão e aprimoramento contínuo do artefato.

Para orientar a execução da pesquisa de forma sistemática, adota-se o modelo processual de [6], que organiza a DSR em seis etapas: (*i*) identificação do problema e motivação; (*ii*) definição dos objetivos da solução; (*iii*) design e desenvolvimento; (*iv*) demonstração; (*v*) avaliação; e (*vi*) comunicação. As etapas foram conduzidas de forma sequencial e iterativa.

4.3.1.1. Identificação do Problema

Na fase de identificação do problema e motivação, constatou-se que, no contexto da administração pública, há carência de soluções integradas e automatizadas para o Gerenciamento de Eventos de TI, o que compromete a detecção ágil, a classificação precisa e a resposta tempestiva a incidentes [90], [24]. A literatura recente indica que o gerenciamento de alertas e incidentes permanece amplamente manual e carece de uma arquitetura uniforme que integre todo o ciclo, do monitoramento à resolução [15].

4.3.1.2. Definição dos Objetivos da Solução

Na etapa de definição dos objetivos, guiada pelos princípios do ITIL 4, foram estabelecidos como metas: (*i*) automatizar o fluxo de MGE; (*ii*) integrar ferramentas *open source* de monitoramento, processamento intermediário e gestão de serviços; (*iii*) aumentar a granularidade da classificação de eventos; e (*iv*) assegurar aderência às melhores práticas de governança e gestão de serviços de TI.

4.3.1.3. Design e Construção do Artefato

O design e desenvolvimento do artefato foi modelado em BPMN 2.0 [31], especificando as interações entre três componentes principais: (*i*) ZABBIX, responsável pelo monitoramento em tempo real e envio de eventos; (*ii*) MIF, módulo intermediário que recebe o evento e aplica uma matriz de criticidade Fuzzy com funções de pertinência e regras linguísticas baseadas em [2], [4], [3] e em modelos de risco de LF de [91], [40]; e (*iii*) GLPI, acessado por *Representational State Transfer Application Programming Interface* (*API REST)*, que registra ou atualiza o *ticket* conforme a prioridade calculada.

Para evitar duplicidade de *tickets*, o MIF mantém um log dos eventos processados e descarta repetições subsequentes.

4.3.1.4. Demonstração

A demonstração foi realizada em ambiente piloto com ativos em produção, utilizando um switch de distribuição real, identificado pelo codinome “BORDA-02” para preservar a confidencialidade da infraestrutura municipal. O evento de interrupção, seguido da restauração do *link*, foi tratado integralmente pelo fluxo ZABBIX, Matriz de Inferência Fuzzy (MIF) e GLPI, permitindo validar a automação completa do processo de abertura e encerramento de *tickets* sem exposição de dados operacionais sensíveis.

4.3.1.5. Avaliação

A etapa de avaliação deste estudo abrangeu tanto a avaliação institucional quanto a avaliação técnica, contemplando uma análise comparativa entre o cenário anterior à implantação e o modelo proposto para o gerenciamento automatizado de eventos.

No âmbito da avaliação institucional, examinou-se o nível de maturidade pré-implantação em governança de TIC utilizando o modelo GAIA, aplicado por meio da ferramenta [55]. Essa avaliação permitiu identificar lacunas estruturais de padronização, rastreabilidade e coordenação operacional que contextualizam o ambiente no qual o artefato seria aplicado.

Em complemento, a avaliação técnica concentrou-se nos indicadores operacionais do sistema legado, possibilitando estabelecer a linha de base quantitativa necessária para comparar o desempenho do modelo automatizado.

Essa análise envolveu a extração e o tratamento dos registros históricos, bem como o cálculo dos indicadores de MTTD e MTTR, fornecendo parâmetros objetivos para mensurar a eficiência do fluxo de detecção e resposta antes da implantação da solução proposta.

No cenário pré-implantação, os registros de incidentes são realizados manualmente por meio do sistema legado *open source* de gestão de demandas OCOMON, o que resulta em detecção apenas após a ocorrência de degradação perceptível dos serviços.

Foram extraídos e tratados os dados do sistema legado referente aos últimos 90 dias pré-implantação. O cálculo dos indicadores quantitativos de MTTD e MTTR foi realizado conforme as práticas recomendadas por [1] e [51] e conforme exigido por [50] por

meio da diferença entre os registros de data e hora de abertura, atendimento e encerramento dos *tickets* de incidente.

Diante desse cenário, a Equação (1) apresenta a formalização do cálculo do MTTD conforme aplicado ao sistema legado, permitindo mensurar o tempo médio de detecção de incidentes a partir dos registros históricos disponíveis:

$$MTTD = \frac{\sum (t_{det} - t_{abr})}{n} \quad (1)$$

Sendo:

$MTTD$ = tempo médio de detecção;

t_{det} = momento de detecção do incidente;

t_{abr} = momento de abertura do *ticket*;

n = quantidade total de incidentes considerados.

Na sequência, a Equação (2) estabelece a metodologia para o cálculo do MTTR, possibilitando a quantificação do tempo médio necessário para a resolução de incidentes no ambiente analisado, a partir dos dados registrados no sistema legado:

$$MTTD = \frac{\sum (t_{res} - t_{abr})}{n} \quad (2)$$

Sendo:

$MTTD$ = tempo médio de detecção;

t_{res} = momento de resolução do incidente;

t_{abr} = momento de abertura do *ticket*;

n = quantidade total de incidentes considerados.

Essas métricas permitem estabelecer uma linha de base quantitativa do sistema legado em produção e criar parâmetros comparativos robustos para avaliar ganhos após a implantação do modelo proposto.

Cabe destacar que, por se tratar de um projeto piloto, a avaliação quantitativa do impacto do novo modelo será conduzida em trabalhos futuros, após a implantação e estabilização do fluxo automatizado.

Desta forma, a metodologia aplicada nesta etapa estabelece a linha de base para comparação, permitindo monitorar e mensurar os ganhos efetivos de desempenho e maturidade na gestão de eventos de TI em avaliações subsequentes.

4.3.1.6. Comunicação

A etapa de comunicação consistiu na sistematização e divulgação dos procedimentos metodológicos, do artefato desenvolvido e dos resultados obtidos, em conformidade com as diretrizes do DSR. Essa etapa assegura que o conhecimento produzido seja acessível a pesquisadores, gestores públicos e profissionais de TI interessados em soluções automatizadas para o Gerenciamento de Eventos.

A comunicação formal dos resultados ocorreu por meio desta dissertação e da documentação técnica associada, que descreve o modelo proposto e os parâmetros operacionais necessários para implantação do artefato.

Complementarmente, os achados foram consolidados em artigos submetidos a eventos científicos da área de Sistemas de Informação e Governança de TIC, ampliando o alcance e a visibilidade do estudo.

Para garantir transparência e replicabilidade, disponibilizou-se um repositório digital contendo os códigos-fonte, arquivos de configuração, exemplos de execução e instruções detalhadas para reprodução do modelo de automação do MGE.

Esse repositório permite que outras instituições repliquem, adaptem ou evoluam o artefato, fortalecendo a contribuição científica e prática da pesquisa. público.

4.3.1.7. Quadro-Resumo da Aplicação DSR

A Tabela 2, a seguir, sintetiza os principais elementos da aplicação do método DSR neste estudo, reunindo o problema, o artefato desenvolvido, o ambiente de aplicação e a forma de avaliação adotada.

Tabela 2 - Síntese da Aplicação do Método DSR

Elemento	Descrição
Problema	Ausência de um modelo integrado e automatizado de MGE capaz de unificar detecção, classificação adaptativa de criticidade e abertura/fechamento de *tickets*,

	resultando em elevado MTTD, MTTR e baixa padronização operacional em ambientes municipais.
Artefato	Arquitetura aberta composta por: (*i*) fluxo BPMN alinhado à prática de MGE do ITIL 4; (*ii*) integração entre Zabbix, Motor de Inferência Fuzzy em Python e GLPI; (*iii*) matriz de criticidade Fuzzy; (*iv*) mecanismos de correlação, idempotência e atualização automática de *tickets*; (*v*) repositório digital para replicabilidade.
Ambiente	Prefeitura Municipal de Arapongas, em ambiente piloto segregado, alimentado com dados reais da infraestrutura municipal, caracterizada por rede de alta complexidade, múltiplos ativos críticos e operações contínuas de serviços públicos digitais.
Forma de Avaliação	visando identificar o nível de maturidade pré-implantação, e avaliação técnica baseada na linha de base quantitativa do sistema legado, com análise dos indicadores MTTD e MTTR no período anterior à implantação, complementada pela demonstração da viabilidade técnica do modelo em ambiente piloto.

4.4. Metodologia do Projeto

Esta subseção descreve a abordagem prática adotada para a execução do projeto, detalhando o contexto institucional, a infraestrutura tecnológica disponível e os elementos que sustentaram o desenvolvimento e a validação do modelo proposto de MGE.

4.4.1. Âmbito e Contexto da Aplicação

O estudo foi desenvolvido na Prefeitura Municipal de Arapongas, localizada no norte do Estado do Paraná, integrante da Região Metropolitana de Londrina, que completou 78 anos de fundação em 2025.

Segundo o Instituto Brasileiro de Geografia e Estatística (IBGE)[3], o município possui área territorial de aproximadamente 400.000 km² e população estimada em 124 838 habitantes (2025), com densidade demográfica de cerca de 311,7 hab/km². Classificado pelo IBGE como município GP1A (de 100.001 até 300.000 habitantes), considerado de grande porte para fins de políticas públicas.

Arapongas consolidou-se como importante polo moveleiro e industrial, com crescente demanda por serviços públicos digitalizados e infraestrutura tecnológica de suporte

[3] Disponível em: https://www.mds.gov.br/webarquivos/arquivo/assistencia_social/suas10anos_2015.pdf

às atividades administrativas. A área de Tecnologia da Informação (TI) da prefeitura sustenta todos os sistemas essenciais das secretarias municipais, formando a base empírica desta pesquisa.

A Diretoria de Tecnologia da Informação (DTI) mantém uma infraestrutura de rede de dados de alta complexidade, composta por aproximadamente 64,3 quilômetros de fibra óptica própria, que interliga secretarias, unidades administrativas e prédios públicos.

A rede é complementada por *links* redundantes de transporte contratados de provedores externos, garantindo continuidade operacional para sistemas críticos. Além disso, torres autossustentadas distribuídas pelo território municipal provêm *uplink* a regiões rurais e unidades descentralizadas, assegurando conectividade mesmo em áreas distantes do núcleo urbano.

Todos os pontos de acesso utilizam switches gerenciáveis, permitindo controle granular de *Virtual Local Area Network* (VLANs) e monitoramento em nível de enlace e dispositivo. A combinação de ativos heterogêneos, tráfego elevado e interdependência entre serviços produz um volume significativo de métricas e eventos operacionais, configurando um laboratório ideal para estudos de monitoração e correlação automatizada.

Apesar da maturidade da infraestrutura, os mecanismos existentes de monitoramento e resposta apresentavam limitações, com práticas pouco padronizadas de correlação de alertas, classificação de incidentes e escalonamento. A ausência de um fluxo institucionalizado de MGE reforçou a pertinência de avaliar um artefato alinhado às práticas preconizadas pela ITIL 4, integrando ZABBIX (monitoração), Motor Fuzzy em Python (classificação adaptativa) e GLPI (gestão de *tickets*).

Inserir o estudo nesse contexto possibilitou validar o modelo proposto em ambiente real de produção, contribuindo para o aperfeiçoamento da governança de TIC e para o aumento da confiabilidade e continuidade dos serviços digitais ofertados à população.

4.4.2. Arquitetura Tecnológica Empregada

A arquitetura tecnológica proposta integra três módulos principais, organizados de forma modular para garantir interoperabilidade, flexibilidade e rastreabilidade ao processo de MGE.

O primeiro módulo é o ZABBIX, responsável pela coleta contínua de métricas, detecção de anomalias e geração de eventos em tempo real. Sua capacidade de

instrumentação por agentes, SNMP e verificações remotas possibilita observação granular do desempenho dos ativos críticos da infraestrutura municipal.

O segundo módulo é o Motor de Inferência Fuzzy (MIF), desenvolvido em Python, que executa a classificação adaptativa dos eventos. O MIF utiliza uma matriz 5x5 baseada nos eixos impacto e urgência, aplicando funções de pertinência, regras de inferência e defuzzificação para produzir valores contínuos convertidos em níveis linguísticos de criticidade. Um arquivo externo de configuração atua como mapa de decisão, permitindo ajustes de regras e comportamento sem alterações no código-fonte.

O terceiro módulo é o GLPI, empregado como plataforma de gestão de serviços para abertura, priorização, atualização e encerramento automatizado de *tickets*. A comunicação entre o MIF e o GLPI ocorre por meio de *APIs REST*, assegurando integração estável e registro completo do ciclo de vida dos incidentes.

Os módulos interagem por meio de *webhooks* e mensagens estruturadas em *JSON*. Essa organização modular reduz a dependência entre componentes, facilita a manutenção e permite adaptar o modelo a diferentes cenários institucionais sem reestruturações profundas.

4.4.3. Etapas Operacionais da Implementação

A implementação do modelo ocorreu em etapas estruturadas, permitindo validar o funcionamento do artefato e ajustar sua operação em ambiente real.

- Configuração do ambiente piloto: Instâncias dedicadas do ZABBIX e do GLPI foram instaladas em ambiente isolado, porém alimentadas por dados reais provenientes da infraestrutura municipal;
- Modelagem dos fluxos em BPMN: Foram construídos diagramas formais representando o processo completo de MGE, incluindo deteção de eventos, classificação, decisões de tratamento e encerramento. Os fluxos em BPMN orientaram a lógica de implementação e estabeleceram as regras operacionais do modelo;
- Desenvolvimento do Motor Fuzzy: O MIF foi implementado com base em funções de pertinência e regras de inferência determinadas pela matriz multicritério. Foram incluídos mecanismos de idempotência para prevenir duplicidade de *tickets*, considerando a possibilidade de retransmissão de eventos pelo ZABBIX;

- Integração entre os módulos: Rotinas e mecanismos de integração foram implementados para assegurar o fluxo completo entre as ferramentas *open source*, permitindo a comunicação entre o ZABBIX, o Motor de Inferência Fuzzy e o GLPI.
- Execução do piloto: Com a integração consolidada, o modelo operou de forma contínua, processando eventos reais relacionados a servidores, enlaces e serviços críticos. Essa etapa forneceu evidências sobre desempenho, consistência e aderência ao fluxo BPMN modelado.

Essas etapas permitiram demonstrar a viabilidade prática do modelo e produzir evidências empíricas essenciais para avaliação técnica e discussão dos resultados.

4.4.4. Critérios Práticos de Avaliação

A avaliação prática do artefato baseou-se em critérios técnicos definidos para aferir sua precisão, estabilidade e aderência ao fluxo modelado.

O primeiro critério foi a coerência da classificação Fuzzy, verificando se os níveis de criticidade previstos pelo MIF, conforme definidos na matriz multicritério e ilustrados nas tabelas do modelo, apresentam consistência lógica em relação às dimensões de impacto e urgência, considerando que sua aplicação em ambiente operacional ainda se encontra em fase inicial de validação.

O segundo critério avaliou a acurácia da automação de *tickets*, considerando a correta abertura, atualização e encerramento dos chamados no GLPI, inclusive em situações de exceção, eventos repetidos e oscilações de métricas.

Também foi analisado o comportamento da idempotência, essencial para evitar múltiplos registros provenientes de um mesmo evento em casos de retransmissão ou instabilidade na entrega dos *webhooks*. A robustez desse mecanismo foi verificada pela ausência de duplicidades durante a execução do piloto.

Outro critério relevante foi a rastreabilidade das ações, garantindo que cada evento pudesse ser acompanhado desde sua origem no ZABBIX até o encerramento do ticket no GLPI. Essa rastreabilidade permitiu avaliar a transparência operacional do modelo.

Por fim, verificou-se a aderência operacional ao fluxo BPMN, assegurando que o comportamento do sistema estivesse alinhado às regras e decisões estabelecidas no

processo formalizado, fornecendo assim, uma base sólida para analisar a eficácia do artefato e estabelecer sua contribuição para a gestão de eventos de TIC no contexto municipal.

5. DESCRIÇÃO DO MODELO PROPOSTO

Apresenta-se, neste capítulo a descrição do modelo proposto para a MGE em TIC no contexto do setor público municipal. Contempla a explicação dos fluxos operacionais desenvolvidos, fundamentados nas melhores práticas da ITIL 4 e modelados com a notação BPMN, evidenciando as etapas, decisões, interações entre os agentes e a decomposição dos processos.

O modelo completo está disponibilizado no endereço[4], no qual se encontram os artefatos em notação BPMN que documentam: (*i*) a arquitetura global do fluxo de Monitoração e Gerenciamento de Eventos; (*ii*) os atores institucionais e suas respectivas atribuições de responsabilidade; (*iii*) as fases operacionais desdobradas em dois níveis de granularidade (implementação plena e configuração mínima), evidenciando os procedimentos críticos para adoção inicial; (*iv*) os recursos tecnológicos e organizacionais necessários à execução do fluxo; e (*v*) as correspondências Entrada/Ação/Saída, que asseguram rastreabilidade integral das decisões e dos produtos gerados em cada etapa do processo.

O repositório inclui, ainda, cinco fluxos em BPMN específicos: (*i*) Fluxo MGE Automático Completo, que descreve a orquestração *end-to-end* entre Zabbix, MIF e GLPI sem intervenção humana; (*ii*) Fluxo MGE Manual, concebido para validação por operadores; (*iii*) Fluxo Plano de Monitoração, que disciplina a elaboração e a revisão periódica de métricas, limiares e regras de correlação; (*iv*) Fluxo Monitorar, responsável pela execução rotineira das tarefas e observação contínua, com o objetivo de identificar variações, desvios ou comportamentos anômalos que possam gerar eventos; e (v*)* MGE Automático para Eventos (apenas exceção), focado no tratamento imediato de ocorrências críticas, disponibilizando atalhos que aceleram a priorização e o escalonamento, podendo ser utilizado como alternativa para instituições com nível de maturidade muito baixa ou baixa em governança de TIC.

Além da descrição dos fluxos, este capítulo examina a infraestrutura tecnológica que sustenta o artefato, enfatizando a interação de três módulos centrais. O Zabbix atua como plataforma de monitoração contínua, coletando métricas e gerando eventos em tempo real. Esses registros são processados pelo Motor de Inferência Fuzzy (MIF), desenvolvido em Python e parametrizado por uma matriz multicritério 5 x 5 baseada nos eixos de impacto e urgência, esse mecanismo constitui o núcleo analítico do modelo, atribuindo níveis

[4] Modelo de Monitoração e Gerenciamento de Evento em BPMN. Disponível em: [https://governanca.arapongas.pr.gov.br/gmon/#list]. Acesso em: 31 mar. de 2026.

graduais de criticidade aos eventos. Os resultados da inferência Fuzzy alimentam o GLPI, que automatiza a abertura, a atualização e o encerramento de *tickets*, garantindo rastreabilidade integral e fechamento eficaz do ciclo de tratamento de incidentes.

5.3. O Fluxo MGE Completo Automatizado

O modelo proposto foi concebido para garantir continuidade, padronização e tratamento proporcional dos eventos de TIC. Em vez de atuar apenas de forma reativa, ou seja, somente após a ocorrência de um evento, sem antecipação, o modelo antecipa falhas, ajusta o nível de resposta conforme a criticidade e reforça a governança de serviços segundo as diretrizes do ITIL 4 [1].

A Figura 1, apresentada a seguir, consolida uma visão geral das etapas essenciais do fluxo automatizado de MGE, evidenciando os principais pontos de decisão e de transição entre as fases do processo.

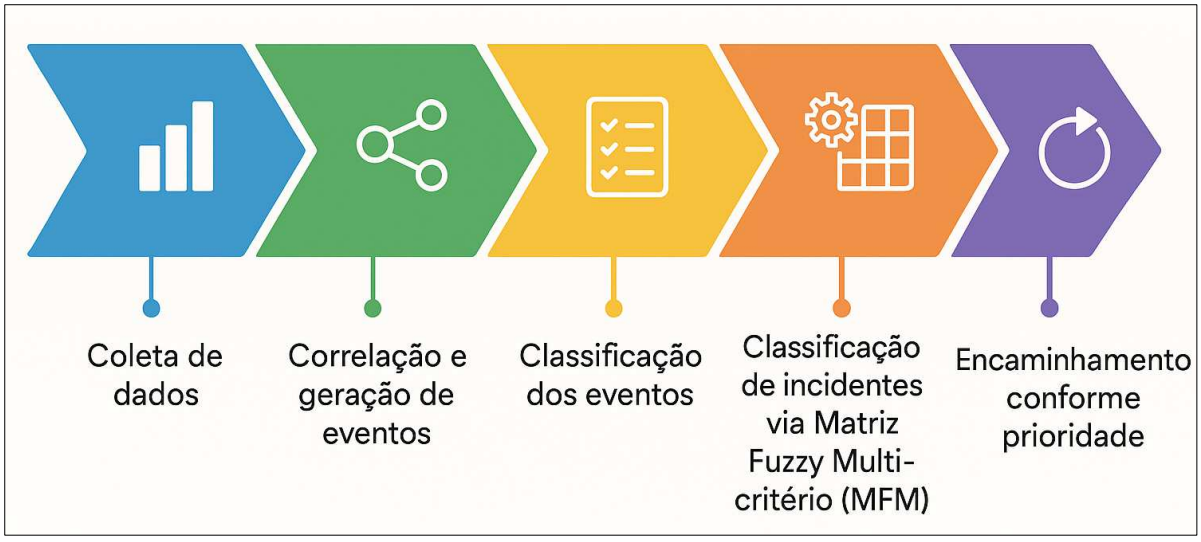


Figura 1 - Etapas de execução do fluxo de MGE. Fonte: Autor.

A execução do GAIA-MGE compreende etapas estruturadas que asseguram o monitoramento contínuo, a análise inteligente e o tratamento eficiente dos eventos. As principais fases do processo são descritas a seguir:

- Coleta de dados: inicia-se com a obtenção contínua de métricas, registros de logs e demais informações operacionais dos ativos monitorados;

- Correlação e geração de eventos: os dados reunidos são analisados em busca de padrões de comportamento, resultando na emissão de eventos que refletem o estado do ambiente;
- Classificação dos eventos: cada evento é enquadrado em uma das categorias: (*i*) Informativo (usado apenas para auditoria e histórico). (*ii*) Alerta: requer atenção e pode demandar ação. (*iii*) Exceção: aponta situações anômalas ou críticas;
- Classificação de incidentes via Matriz Fuzzy Multicritério (MFMC): para alertas e exceções, aplica-se a MFMC, que avalia os critérios de impacto e urgência, atribuindo um nível de prioridade de forma contextualizada e mais refinada que abordagens binárias tradicionais;
- Encaminhamento conforme prioridade: Baixa (registra-se no histórico ou abre-se *ticket* técnico para monitoramento contínuo), Média (categoriza-se o evento, inicia-se a abertura de *ticket* e direciona-se para gerenciamento de incidentes ou problemas), Alta (inicia-se a abertura de *ticket* e acionam-se imediatamente ações corretivas, realiza análise de impacto e encaminha para ação de contorno e se necessário, direciona ao processo formal de incidentes ou problemas, sempre documentando via *ticket*.

A Figura 2, apresenta o fluxo completo de MGE, desenvolvido em notação BPMN. O diagrama organiza, de forma lógica e sequencial, as etapas do processo, abrangendo desde o monitoramento contínuo dos ativos até o encaminhamento das ações corretivas correspondentes.

O modelo fundamenta-se em um fluxo processual estruturado que integra monitoramento contínuo, análise inteligente de eventos e priorização dinâmica de incidentes. Essa abordagem busca alinhar a gestão de eventos às práticas de governança de TIC preconizadas pelo ITIL 4, promovendo respostas mais ágeis, consistentes e orientadas por evidências.

O fluxo proposto visa fortalecer a capacidade institucional de resposta a eventos, ampliando a resiliência, a rastreabilidade e a qualidade dos serviços prestados. Além disso, sua adoção contribui para o avanço da maturidade organizacional, possibilitando a geração de indicadores de desempenho, auditorias de conformidade, análises de tendência e a melhoria contínua dos processos de suporte.

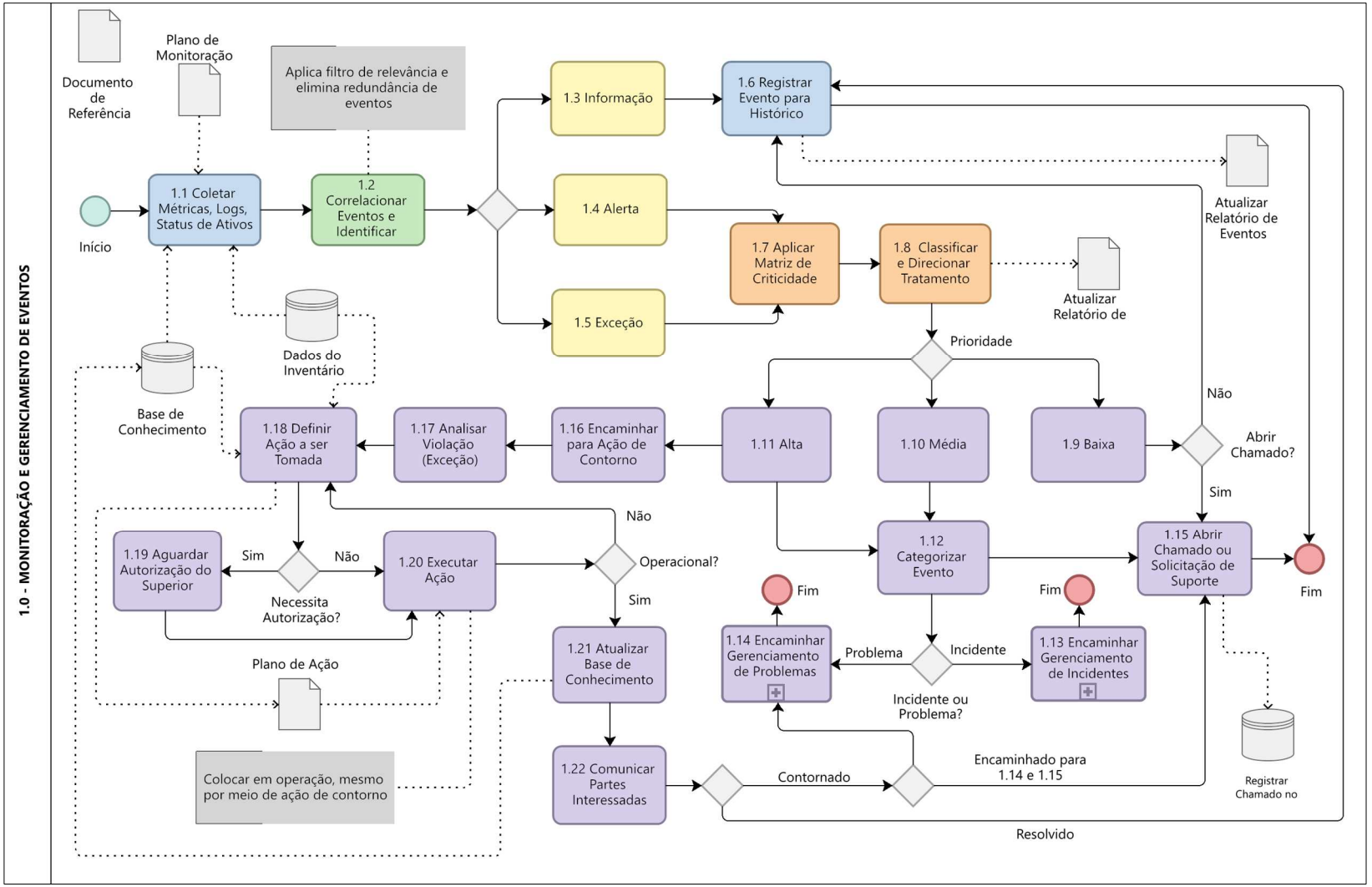


Figura 2 - Representação em BPMN do MGE. Legenda de cores: Azul claro = coleta/registro; Verde claro = correlação/identificação; Amarelo claro = classificação; Laranja claro = avaliação/priorização; Roxo claro = decisão/ação. Autor.

A Tabela 3, apresenta a decomposição detalhada do fluxo ilustrado na Figura 1, contemplando todas as etapas do processo, do item 1.1 ao 1.22. A tabela consolida a documentação estruturada de cada fase, incluindo informações como objetivos, responsáveis, entradas, saídas e descrições das tarefas, assegurando rigor metodológico, transparência na execução e possibilita uma análise aprofundada das atividades que compõem o modelo operacional.

Tabela 3 - Decomposição MGE automatizado

1.1 Coletar Métricas, Logs, Status de Ativos	
Objetivo: Captar dados operacionais e de desempenho dos ativos de TI para subsidiar a análise de eventos.	**Descrição das Tarefas:** ● Nesta etapa, realiza-se a coleta das informações operacionais dos ativos monitorados, incluindo métricas de desempenho, registros de log e status de funcionamento. Essa etapa é essencial para alimentar o processo de correlação e análise de eventos subsequentes, garantindo uma base informacional consistente e atualizada.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Plano de Monitoramento, Base de Conhecimento, Inventário de Ativos.	
Saídas: Conjunto de dados coletados sobre os ativos monitorados (métricas, logs, status).	
1.2 Correlacionar Eventos e Identificar Padrões	
Objetivo: Identificar padrões e relações entre eventos para reduzir ruídos e facilitar a classificação.	**Descrição das Tarefas:** ● Nesta etapa, os dados coletados são organizados e cruzados para identificar ocorrências repetitivas, relações causais e possíveis padrões de comportamento anômalo. O objetivo é reduzir redundâncias, eliminar falsos positivos e preparar o evento para sua devida classificação no fluxo.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Dados coletados dos ativos (métricas, logs, status), histórico de eventos.	
Saídas: Eventos organizados e filtrados, prontos para classificação por tipo.	
1.3 Informativo	
Objetivo: Registrar eventos que indicam o funcionamento esperado ou alterações sem impacto.	**Descrição das Tarefas:** ● Eventos do tipo informativo são tratados de forma passiva, sendo registrados apenas para rastreabilidade, sem a necessidade de resposta imediata.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Evento classificado como informativo (ex: logs de rotina, confirmações de execução).	
Saídas: Evento registrado no histórico para fins de auditoria e análise futura.	
1.4 Alerta	
Objetivo: Identificar situações que exigem atenção, mas que ainda não representam falhas.	**Descrição das Tarefas:** ● Alertas indicam condições que podem evoluir para falhas, exigindo análise para definir se ações preventivas são necessárias.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Evento com sinal de anomalia ou aproximação de limites operacionais.	
Saídas Encaminhamento para avaliação de impacto e urgência (1.7).	
1.5 Exceção	
Objetivo: Reconhecer eventos que	**Descrição das Tarefas:**

representam falhas, indisponibilidades ou violações críticas. **Responsável:** Equipe técnica da Diretoria de TI. **Entradas:** Evento anômalo detectado com impacto direto nos serviços de TI. **Saídas:** Encaminhamento para avaliação de impacto e urgência (1.7).	● Eventos classificados como exceção indicam interrupções ou falhas em andamento e exigem resposta imediata conforme prioridade.
1.6 Registrar Evento para Histórico	
Objetivo: Documentar eventos para fins de rastreabilidade, auditoria e análise futura. **Responsável:** Equipe técnica da Diretoria de TI. **Entradas:** Evento classificado como informativo ou de baixa prioridade. **Saídas:** Registro arquivado no banco de dados da ferramenta de monitoramento.	**Descrição das Tarefas:** ● Nesta etapa, o evento é formalmente registrado no sistema, mesmo que não exija ação corretiva, garantindo histórico confiável para consultas, estatísticas e melhorias contínuas.
1.7 Aplicar Matriz de Criticidade	
Objetivo: Determinar a prioridade do evento com base na avaliação de impacto e urgência. **Responsável:** Equipe técnica da Diretoria de TI. **Entradas:** Evento classificado como alerta ou exceção; critérios da matriz; dados do inventário. **Saídas:** Evento classificado como prioridade baixa, média ou alta.	**Descrição das Tarefas:** ● Esta etapa utiliza uma matriz para cruzar impacto e urgência, atribuindo um nível de prioridade que orientará o tratamento adequado do evento.
1.8 Classificar e Direcionar Tratamento	
Objetivo: Encaminhar o evento para o fluxo apropriado com base na prioridade atribuída. **Responsável:** Equipe técnica da Diretoria de TI. **Entradas:** Evento com prioridade definida (baixa, média ou alta) após aplicação da matriz de criticidade. **Saídas:** Evento encaminhado para os fluxos correspondentes: 1.9 (Baixa), 1.10 (Média) ou 1.11 (Alta).	**Descrição das Tarefas:** ● Com base na criticidade atribuída, o evento é direcionado para o tratamento adequado, assegurando resposta compatível com o grau de risco ou impacto.
1.9 Baixa	
Objetivo: Definir se o evento de baixa prioridade requer abertura de chamado ou apenas registro histórico. **Responsável:** Equipe técnica da Diretoria de TI. **Entradas:** Evento classificado como prioridade baixa. **Saídas:** Encaminhamento para 1.6 (Registro no histórico) ou 1.15 (Abertura de chamado).	**Descrição das Tarefas:** ● Eventos de baixa prioridade são analisados para verificar a necessidade de intervenção. Se não exigirem ação imediata, são apenas registrados. Caso contrário, são formalizados como chamados.
1.10 Média	
Objetivo: Iniciar o tratamento técnico de eventos que exigem resposta, mas sem urgência crítica. **Responsável:** Equipe técnica da Diretoria de TI. **Entradas:** Evento com prioridade média. **Saídas:** Encaminhamento para 1.12 Categorizar Evento e, posteriormente, para abertura de chamado.	**Descrição das Tarefas:** ● Eventos com prioridade média são tratados com atenção moderada, seguindo os protocolos definidos para classificação e registro formal no sistema de atendimento.

1.11 Alta	
Objetivo: Iniciar resposta imediata a eventos críticos que impactam significativamente os serviços.	**Descrição das Tarefas:** ● Eventos críticos seguem fluxo emergencial com execução de medidas corretivas imediatas, priorizando o restabelecimento rápido dos serviços e mitigação de danos.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Evento com prioridade alta.	
Saídas: Encaminhamento para 1.16 (Encaminhar para Ação de Contorno) e demais etapas de análise e resposta.	
1.12 Categorizar Evento	
Objetivo: Classificar o evento como incidente ou problema, conforme sua natureza e recorrência.	**Descrição das Tarefas:** ● Com base nas características do evento, é feita a categorização para definir se o evento é incidente ou problema.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Evento de prioridade média ou alta; histórico de eventos e regras de categorização.	
Saídas: Encaminhamento para 1.13 (Incidente) ou 1.14 (Problema).	
1.13 Encaminhar Gerenciamento de Incidentes	
Objetivo: Ativar o processo de Gerenciamento de Incidentes para resolução rápida de falhas.	**Descrição das Tarefas:** ● Eventos tratados como incidentes seguem protocolo de atendimento técnico, esta etapa se integra ao fluxo específico de incidentes da instituição.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Evento classificado como incidente.	
Saídas: Evento tratado segundo os procedimentos definidos no fluxo de incidentes.	
1.14 Encaminhar Gerenciamento de Problemas	
Objetivo: Encaminhar o evento para investigação da causa raiz, conforme processo de problemas.	**Descrição das Tarefas:** ● Eventos recorrentes ou com causas desconhecidas são tratados como problemas e direcionados para investigação estruturada, conforme o fluxo específico de Problemas.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Evento classificado como problema.	
Saídas: Evento tratado segundo os procedimentos definidos no fluxo de problemas.	
1.15 Abrir Chamado ou Solicitação de Suporte	
Objetivo: Registrar formalmente a demanda técnica no sistema de atendimento, permitindo seu acompanhamento e tratamento.	**Descrição das Tarefas:** ● A abertura do chamado formaliza o atendimento à ocorrência registrada, permitindo rastreabilidade, atribuição de prioridade e encaminhamento para a equipe responsável.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Evento com necessidade de acompanhamento técnico (proveniente de classificações anteriores ou encaminhamento direto).	
Saídas: Chamado aberto no sistema (ex: ISTM ou ferramenta equivalente) com status definido e responsável atribuído.	
1.16 Encaminhar para Ação de Contorno	
Objetivo: Garantir a continuidade operacional dos serviços por meio de medidas temporárias enquanto a solução definitiva é analisada.	**Descrição das Tarefas:** ● Nesta etapa, aplica-se uma ação provisória para mitigar o impacto do evento. A medida visa manter os serviços funcionando enquanto se realiza a análise da violação e a definição da ação definitiva.
Responsável: Equipe técnica da Diretoria de TI.	

Entradas: Evento classificado como de alta prioridade, com impacto imediato.	
Saídas: Execução de ação de contorno e encaminhamento para análise aprofundada (1.17).	
1.17 Analisar Violação (Exceção)	
Objetivo: Avaliar tecnicamente a exceção detectada, identificando causa, impacto e possíveis recorrências.	**Descrição das Tarefas:** ● A violação é analisada com base em informações técnicas e registros anteriores. O resultado é um relatório com detalhes sobre o ativo afetado, data, hora, tipo de falha e contexto operacional, servindo de base para decisão no item seguinte.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Evento tratado com ação de contorno; dados do inventário, métricas de desempenho e histórico de eventos.	
Saídas: Relatório técnico de incidente/exceção estruturado para orientar a definição da ação.	
1.18 Definir Ação a ser Tomada	
Objetivo: Selecionar a resposta técnica mais adequada com base na análise da exceção e nas informações disponíveis.	**Descrição das Tarefas:** ● Com base nas evidências e histórico, é definida a ação corretiva a ser executada. Avalia-se se a medida requer autorização formal antes da execução, encaminhando o fluxo conforme a decisão.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Relatório técnico da análise (1.17), base de conhecimento, plano de ação pré-definido e inventário de ativos.	
Saídas: Plano de ação definido e decisão sobre necessidade de autorização superior.	
1.19 Aguardar Autorização do Superior	
Objetivo: Suspender temporariamente a execução da ação até que seja obtida autorização formal da autoridade competente.	**Descrição das Tarefas:** ● Se a ação planejada envolver risco, impacto significativo ou estiver fora dos parâmetros de autonomia da equipe técnica, é solicitada autorização superior. O fluxo é retomado apenas após a aprovação.
Responsável: Diretor/Gerente/Coordenador de TI.	
Entradas: Plano de ação definido no item 1.18, classificado como ação que requer aprovação formal (ex: reinício de serviços críticos, aplicação de patch de impacto).	
Saídas: Autorização formal registrada e liberação para continuidade do fluxo (item 1.20).	
1.20 Executar Ação	
Objetivo: Aplicar a ação corretiva ou mitigadora definida, conforme plano aprovado, para restaurar a normalidade operacional.	**Descrição das Tarefas:** ● A equipe executa a ação planejada, como reinicialização de serviço, aplicação de correções ou isolamento de ativo. Em seguida, verifica se o serviço voltou ao funcionamento normal. Caso não tenha surtido efeito, o fluxo retorna ao item 1.18 para reavaliar a solução.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Plano de ação aprovado (com ou sem autorização superior); recursos técnicos disponíveis.	
Saídas: Serviço restaurado ou medida aplicada; verificação de sucesso; decisão sobre continuidade ou reavaliação.	
1.21 Atualizar Base de Conhecimento	
Objetivo: Registrar a solução aplicada, tempo de resposta e lições aprendidas, promovendo aprendizado organizacional e apoio a futuros atendimentos.	**Descrição das Tarefas:** ● As informações da ação executada são documentadas de forma estruturada no repositório de conhecimento da organização (ex.: wiki técnica, sistema de ITSM). Isso inclui soluções definitivas e paliativas, contribuindo para o
Responsável: Equipe técnica da Diretoria de	

TI.	histórico de suporte e resolução de problemas.
Entradas: Dados da ação executada (item 1.20), resultado da intervenção, relatórios técnicos.	
Saídas: Registro atualizado na base de conhecimento com evidências e classificações adequadas.	
1.22 Comunicar Partes Interessadas	
Objetivo: Garantir que usuários, áreas de negócio e demais envolvidos estejam cientes da ocorrência, ação tomada e status final do evento.	**Descrição das Tarefas:** ● Nesta etapa, o evento é formalmente registrado no sistema, mesmo que não exija ação corretiva, garantindo histórico confiável para consultas, estatísticas e melhorias contínuas.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Relatório final da ação executada, informações da base de conhecimento e status do evento.	
Saídas: Notificações enviadas às partes interessadas; decisão sobre encerramento ou encaminhamento para tratamento de problema.	
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Evento classificado como informativo ou de baixa prioridade.	
Saídas: Registro arquivado no banco de dados da ferramenta de monitoramento.	

5.4. Fluxo de MGE Manual

O fluxo de início manual, representado na Figura 3, refere-se à ativação deliberada do processo de MGE pela equipe técnica responsável pelo monitoramento, sem depender de gatilhos automáticos oriundos do sistema de monitoramento. Trata-se de um procedimento adotado em situações específicas em que se deseja observar de forma proativa um ou mais ativos da infraestrutura de TIC, mesmo que não haja, naquele momento, um alerta gerado automaticamente pela ferramenta de monitoramento (Zabbix).

Esse tipo de acionamento é frequentemente acionado em cenários de auditoria interna, investigações de anomalias operacionais, solicitações formais de acompanhamento institucional, assim como, em ações preventivas planejadas para mitigar riscos de indisponibilidade ou falhas em ativos críticos.

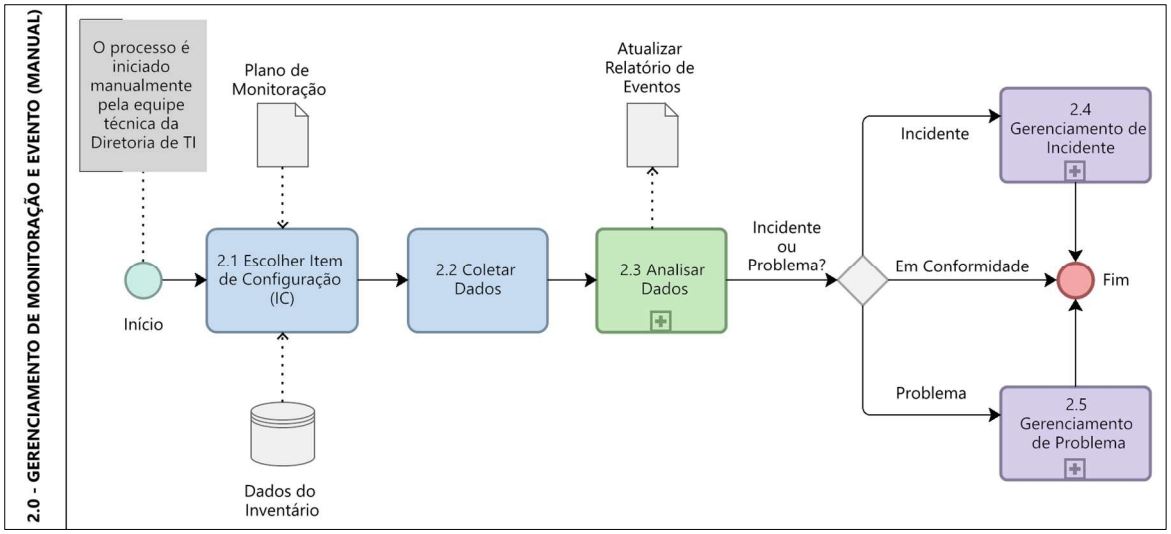


Figura 3 - Fluxo de MGE manual. Fonte: Autor.

O processo segue uma sequência lógica e estruturada, iniciando-se com a seleção do item ou serviço a ser monitorado. Em seguida, realiza-se a coleta ativa de métricas, logs e demais dados operacionais, os quais são analisados com base em critérios técnicos previamente definidos. A partir da análise desses dados, é elaborado um relatório técnico preliminar, que subsidia a decisão da equipe quanto à classificação do evento observado: se trata-se de um incidente em curso, de um problema de causa raiz a ser tratado posteriormente, ou apenas de uma condição operacional normal.

A depender dessa decisão, o fluxo pode seguir por diferentes caminhos: o evento pode ser encerrado e arquivado, caso não haja anormalidades, ou então encaminhado para os fluxos correspondentes de tratamento, como o gerenciamento de incidentes (item 2.4), gerenciamento de problemas (item 2.5).

Essa abordagem manual complementa o monitoramento automatizado contínuo, oferecendo flexibilidade, controle tático e resposta antecipada em situações que requerem atenção personalizada, sendo alinhada aos princípios de melhoria contínua e gestão proativa de riscos previstos nas boas práticas da ITIL 4. A seguir, a Tabela 4, apresenta a descrição detalhada das atividades associadas às etapas (2.1 a 2.5):

Tabela 4 – Decomposição MGE Start Manual

2.1 Escolher Item de Configuração (IC)	
Objetivo: Escolher o IC (item de configuração)	**Descrição das Tarefas:**
Responsável: Equipe técnica da Diretoria de TI.	● Nesta etapa, o analista seleciona qual ativo de TI será monitorado. A escolha é baseada no inventário e no
Entradas: Processo iniciado.	

Acesso ao inventário/planilha e ao plano de monitoração. **Saídas:** Item de Configuração (IC) selecionado. Atividade encaminhada para coleta de dados (2.2).	plano de monitoramento. Trata-se de um passo essencial para direcionar a coleta de dados e garantir que o foco do monitoramento esteja alinhado com os objetivos institucionais.
2.2 Coletar Dados	
Objetivo: Coletar os dados selecionados. **Responsável:** Equipe técnica da Diretoria de TI. - Analista de infraestrutura de TI. **Entradas:** IC selecionado na etapa 2.1. Acesso autorizado ao ativo. **Saídas:** Conjunto de dados coletados (logs, métricas, status); Direcionamento para análise técnica (2.3).	**Descrição das Tarefas:** ● Esta etapa consiste na coleta de dados operacionais e históricos do ativo selecionado, como logs, métricas, status ou alertas anteriores. O objetivo é obter evidências para análise e tomada de decisão na próxima etapa do fluxo.
2.3 Analisar Dados	
Objetivo: Examinar os dados coletados e caso haja necessidade, encaminha para Gerenciamento de Incidente ou Problema. **Responsável:** Equipe técnica da Diretoria de TI. **Entradas:** Lista com os dados selecionados. **Saídas:** Encaminha para Incidente ou Problema, caso haja algum alerta ou retorna relatório e finaliza o processo.	**Descrição das Tarefas:** ● É retornado as informações com os dados coletados e enviado para atualizar relatório de eventos. O fluxo posteriormente pode tomar três diferentes caminhos, sendo eles: 1. O ativo está on-line e com status de "OK": O processo é encerrado; 2. O Ativo é classificado como incidente e direcionado para Invocar o Gerenciamento de Incidentes (2.3), onde o evento é tratado a partir deste fluxo. 3. O Ativo é classificado como problema e direcionado para Invocar Gerenciamento de Problemas (2.4), onde o evento é tratado a partir deste fluxo.
2.4 Gerenciamento de Incidente	
Objetivo: Iniciar processo Gerenciamento de Incidente. **Responsável:** Equipe técnica da Diretoria de TI. **Entradas:** Evento classificado como incidente na etapa 2.3. Indício de falha com impacto direto à operação do serviço de TI ou do usuário final. **Saídas** Evento transferido ao fluxo formal de tratamento de incidentes.	**Descrição das Tarefas:** ● Esta etapa é acionada quando, após análise técnica dos dados coletados (etapa 2.3), o evento é classificado como incidente, ou seja, uma interrupção ou degradação inesperada na qualidade de um serviço de TI que afeta diretamente a operação. O objetivo é restaurar o serviço o mais rápido possível, minimizando o impacto no negócio.
2.5 Gerenciamento de Problema	
Objetivo: Iniciar processo Gerenciamento de Problema. **Responsável:** Equipe técnica da Diretoria de TI. **Entradas:** Evento classificado como problema na etapa 2.3. Situação com recorrência, instabilidade ou degradação sem causa conhecida. **Saídas:** Evento transferido ao fluxo formal de tratamento de problemas.	**Descrição das Tarefas:** ● Esta etapa é acionada quando, após análise técnica dos dados coletados (etapa 2.3), o evento é classificado como problema, ou seja, está relacionado a uma causa raiz não imediata, é recorrente ou revela falhas estruturais no ambiente de TI. O objetivo é iniciar uma investigação mais aprofundada para identificar e eliminar a origem do problema.

5.5. Fluxo do Plano De Monitoração

A efetividade dos processos de monitoramento e gerenciamento de eventos de TI depende não apenas da automação e da padronização operacional, mas também da capacidade institucional de revisar, adaptar e evoluir continuamente suas práticas [1]. Neste contexto, estabelece-se o fluxo de Gerenciamento do Plano de Monitoração, conforme ilustra a

Figura 4, dedicado à avaliação periódica e sistematizada de todo o ciclo de monitoração implementado na organização.

O objetivo consiste em garantir que as estratégias, rotinas e controles implementados permaneçam alinhados às metas organizacionais, respondendo de forma eficaz às transformações do ambiente tecnológico, regulatório e institucional. Essa etapa é essencial para o fortalecimento da governança, o aprimoramento contínuo e a consolidação da maturidade dos processos de gestão de eventos, em conformidade com as melhores práticas internacionais de governança e de gerenciamento de serviços de TIC.

O Fluxo concentra na análise do relatório de eventos e atualização do plano de melhoria. Por meio da condução dessas avaliações, torna-se possível identificar tendências, oportunidades de aprimoramento e pontos de fragilidade no processo, direcionando a construção de planos de ação corretivos e preventivos e assegurando a aderência dos processos às estratégias e exigências institucionais.

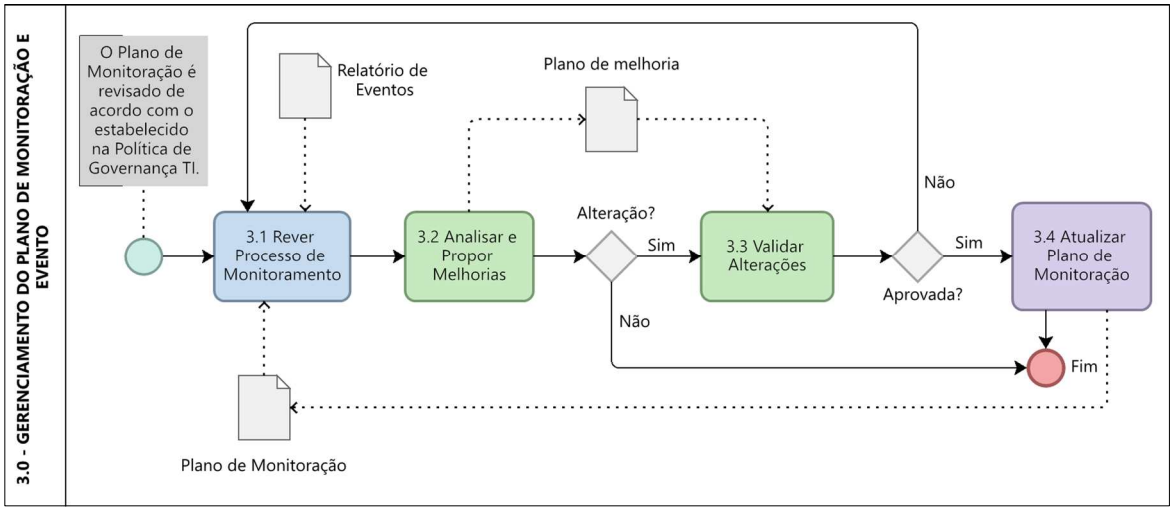


Figura 4 - Fluxo de Gerenciamento do Plano de Monitoração. Fonte: Autor.

A seguir, a Tabela 5, apresenta a descrição detalhada das atividades associadas às etapas (2.1 a 2.5):

Tabela 5 – Decomposição do Plano de Monitoração

3.1 Rever Processo de Monitoramento	
Objetivo: Avaliar periodicamente o processo de monitoração vigente, identificando limitações, falhas ou pontos de melhoria.	**Descrição das Tarefas:** ● Nesta etapa, realiza-se uma revisão crítica do processo de monitoramento vigente, considerando indicadores, falhas recorrentes, efetividade das ações e conformidade com o plano estabelecido.
Responsável: Equipe técnica da Diretoria de TI.	

Entradas: Dados operacionais, indicadores de desempenho, relatórios de eventos e processo atual de MGE.	
Saídas: Diagnóstico do processo atual e base para elaboração de propostas de melhoria (3.2).	
3.2 Analisar e Propor Melhorias	
Objetivo: Produzir um plano de ação com melhorias estruturadas ou validar a continuidade do modelo atual, caso não sejam necessárias alterações.	**Descrição das Tarefas:** ● Com base nas evidências levantadas, avalia-se a necessidade de ajustes no processo de MGE. Se forem identificadas melhorias viáveis, estas são documentadas para validação. Caso o modelo atual esteja adequado, não há alterações.
Responsável: Equipe técnica da Diretoria de TI. - Analista de infraestrutura de TI.	
Entradas: Diagnóstico do processo (3.1), histórico de eventos, indicadores de desempenho e sugestões operacionais.	
Saídas: Caso haja proposta de alteração, o Plano de Melhoria do MGE é encaminhado para validação (3.3). Caso contrário, o processo é encerrado.	
3.3 Validar Alterações	
Objetivo: Revisar e aprovar as melhorias propostas no Plano de Melhoria do MGE.	**Descrição das Tarefas:** ● Nesta etapa ocorre a análise formal da proposta de alteração. A decisão deve considerar custo, viabilidade técnica e aderência ao modelo de governança vigente.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Plano de Melhoria do MGE elaborado (3.2), alinhamento com diretrizes institucionais.	
Saídas: Se aprovado, segue para atualização do plano (3.4). Caso rejeitado, retorna para nova análise (3.2).	
3.4 Atualizar Plano de Monitoração	
Objetivo: Incorporar formalmente as alterações aprovadas ao Plano de Monitoração de Eventos.	**Descrição das Tarefas:** ● Atualizam-se os documentos e artefatos relacionados à monitoração de eventos, refletindo as melhorias aprovadas. O novo plano passa a reger o monitoramento dos serviços de TI da organização.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Plano de melhoria validado (3.3).	
Saídas: Plano de Monitoração atualizado e encerramento do ciclo de revisão.	

5.6. Fluxo Monitorar

A definição clara dos objetivos do monitoramento é fundamental para garantir a eficácia do processo de monitoração e gerenciamento de eventos de TIC, promovendo o alinhamento com as estratégias organizacionais e as necessidades dos usuários finais. Segundo as recomendações da ITIL 4, cabe a cada organização determinar os aspectos que devem ser monitorados, considerando os requisitos do negócio, as expectativas das partes interessadas e o potencial de geração de valor [1].

O fluxo de definição dos objetivos de monitoramento, Figura 5, inicia-se a partir do recebimento de dados essenciais: (*i*) Acordo de Nível de Serviço (ANS), que estabelece padrões mínimos de desempenho e expectativas contratuais; (*ii*) os dados do inventário de ativos, fornecendo a visão sobre os componentes críticos da infraestrutura; (*iii*) os dados de monitoramento em tempo real, que informam sobre o comportamento e a performance dos sistemas; e (*iv*) o próprio plano de monitoração vigente, que orienta as políticas e diretrizes do processo.

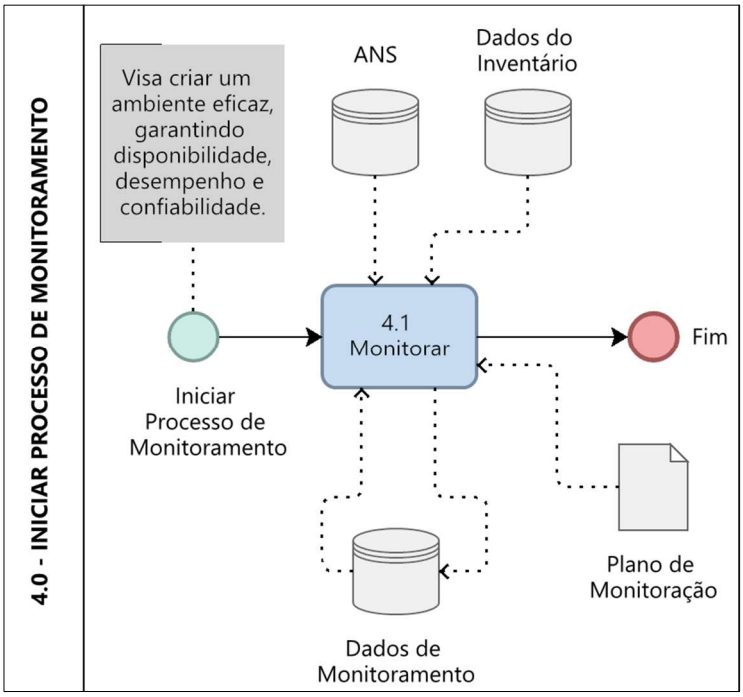


Figura 5 - Fluxo Gerenciamento do Plano de Monitoração. Fonte: Autor.

A seguir, a Tabela 6, apresenta a descrição detalhada das atividades associadas a etapa (4.1):

Tabela 6 – Decomposição do Fluxo Monitorar

4.1 Monitorar	
Objetivo: Realizar a monitoração contínua dos ativos de TI conforme critérios definidos, permitindo a detecção antecipada de desvios, falhas ou degradações.	**Descrição das Tarefas:** ● Executa-se a monitoração ativa e contínua de sistemas, redes e demais ativos críticos. Os dados capturados são armazenados e analisados para identificação automática ou manual de eventos relevantes, servindo de insumo para a tomada de decisão nos fluxos seguintes.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Acordos de Nível de Serviço (ANS), dados do inventário de ativos, plano de monitoração vigente e parâmetros de coleta definidos.	

Saídas: Registros de eventos coletados, indicadores de desempenho e dados de monitoramento enviados aos fluxos de tratamento (informativo, alerta ou exceção).	

5.7. O Fluxo MGE (Evento de Exceção)

A abordagem automatizada representada na Figura 6, é direcionada ao tratamento de eventos de exceção, isto é, alertas críticos e de alto impacto que demandam resposta imediata da equipe de TI, a fim de minimizar riscos à continuidade dos serviços. A adoção desse fluxo específico de exceção mostra-se particularmente adequada para instituições com níveis baixos de maturidade em governança de TIC ou que disponham de recursos operacionais limitados, configurando-se como uma alternativa inicial e gradual ao modelo completo de gerenciamento de eventos.

Essa estratégia permite que a organização inicie a adoção de práticas automatizadas de monitoramento e resposta, mesmo em contextos de estrutura reduzida, concentrando esforços na resposta a chamados de altíssima gravidade. Dessa forma, promove-se um primeiro passo concreto rumo à governança de TIC, fortalecendo a resiliência e a confiabilidade dos serviços e alinhando-se aos princípios de resposta rápida e recuperação definidos pelas melhores práticas da ITIL 4 [1].

Sempre que um incidente classificado como exceção é detectado, torna-se obrigatória a execução de uma ação de contorno, mesmo que provisória, para restabelecer o funcionamento operacional do serviço afetado no menor tempo possível. Caso a primeira tentativa de solução não seja eficaz e o serviço permaneça indisponível, o fluxo prevê a retroalimentação para a etapa de redefinição da ação a ser tomada (etapa 5.2), promovendo ciclos sucessivos de tentativa e análise até que se obtenha, ao menos, a restauração provisória do serviço.

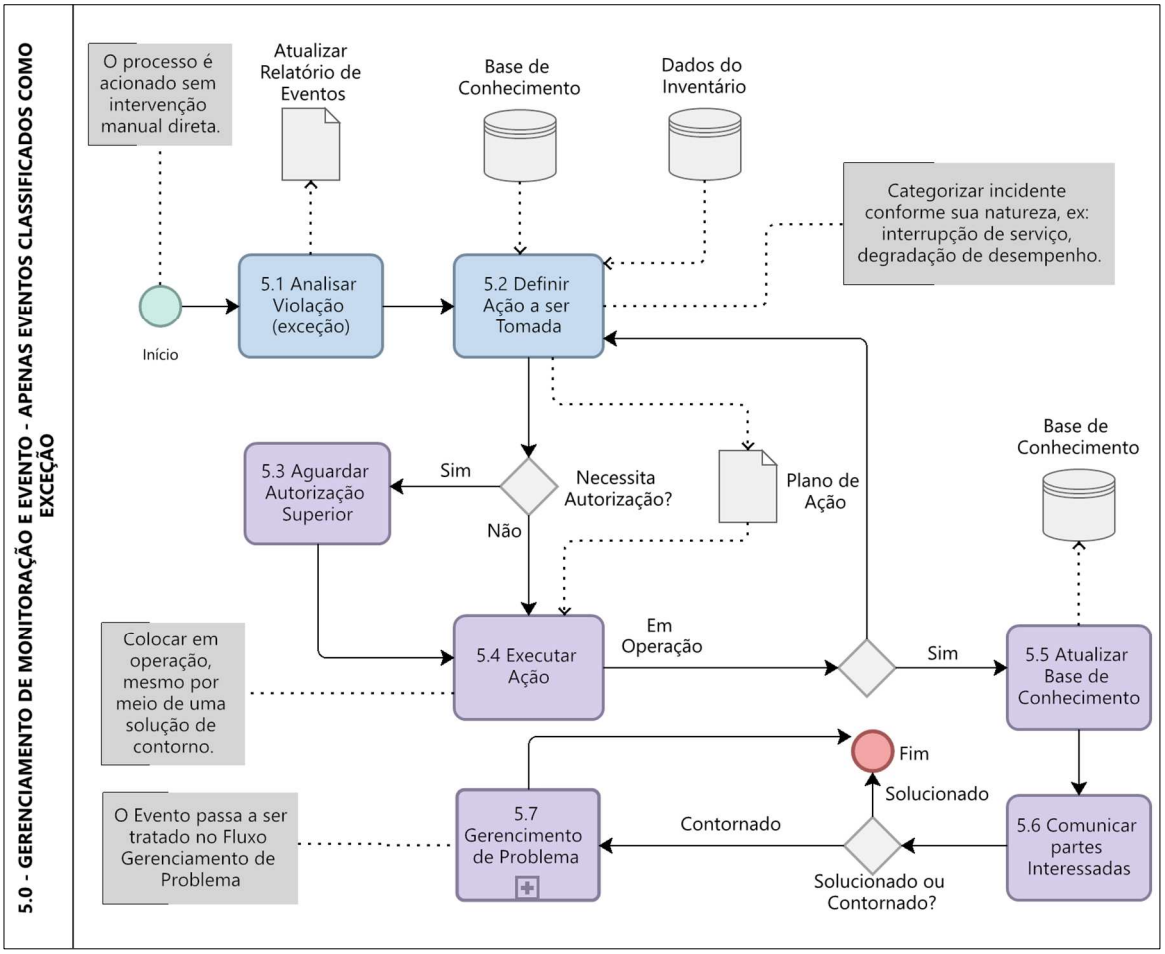


Figura 6 - Fluxo MGE (apenas Exceção). Fonte: Autor.

A seguir, a Tabela 7, apresenta a descrição detalhada das atividades associadas as etapas (5.1 a 5.8):

Tabela 7 – Decomposição do Fluxo MGE (Apenas Exceção)

5.1 Analisar Violação	
Objetivo: Examinar alerta ou violação de serviço.	**Descrição das Tarefas:** ● O processo é acionado sem intervenção manual direta. ● Recebe o relatório com dados de alerta/aviso ou violação de serviço, definido conforme a regra de negócio e encaminha os dados para que sejam categorizados.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Relatório com dados do alerta ou violação.	
Saídas: Encaminha o relatório com análise dos dados para ser categorizado.	
5.2 Categorizar e Definir a Ação a ser Tomada	
Objetivo: Receber os dados analisados e categorizar para que uma ação possa ser definida	**Descrição das Tarefas:** ● O incidente é classificado de acordo com a sua característica e, em seguida, são determinadas as ações a

Responsável: Equipe técnica da Diretoria de TI.	serem tomadas com base na sua gravidade e no impacto que ele tem na disponibilidade dos serviços. ● Recebe dados da Base de Conhecimento e de Dados do Inventário, para que a ação possa ser definida.
Entradas: Reúne as informações do IC com alerta ou violação.	
Saídas: Lista com os dados categorizados.	
5.3 Aguardar Autorização Superior	
Objetivo: Recebe pedido de autorização para que seja executada ação.	**Descrição das Tarefas:** ● Caso seja obrigatório a autorização do superior para a execução da ação, o processo é pausado até autorização do Superior ser concedida. ● Caso contrário, a ação é encaminhada para que seja executada.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Pedido de autorização e relatório do alerta ou violação.	
Saídas: Encaminha relatório com autorização.	
5.4 Executar Ação	
Objetivo: Executar medidas corretivas para resolver o incidente e restaurar os serviços.	**Descrição das Tarefas:** ● Caso o serviço esteja em operação é atualizado o Banco de Dados e comunicado os *stakeholders*. ● Caso o serviço não esteja em operação o processo volta para Categorizar e Definir Ação a ser tomada, pois é obrigatório que uma ação de contorno seja tomada, sendo ela definitiva ou provisória.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Relatório com o Plano de ação de ser tomada.	
Saídas: Ação tomada	
5.5 Atualizar Base de Conhecimento	
Objetivo: Atualizar banco de dados e comunicar *stakeholders*.	**Descrição das Tarefas:** ● É atualizado o Banco de Dados e encaminhado para comunicar os *stakeholders*.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Relatório com ação executada e resultado.	
Saídas:	
5.6 Comunicar Partes Interessadas	
Objetivo: Comunicar os *stakeholders*.	**Descrição das Tarefas:** ● É comunicado os *stakeholders*. ● Caso a ação de contorno tenha solucionado o problema o fluxo é encerro, caso contrário o processo é direcionado para invocar o fluxo de Gerenciamento de Problema.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Relatório de violação e ações tomadas.	
Saídas: não se aplica	
5.7 Gerenciamento de Problema	
Objetivo: Invoca processo Gerenciamento de Problema.	**Descrição das Tarefas:** ● O fluxo de Gerenciamento de Problema é invocado para que o problema possa ser gerenciado pelo novo fluxo.
Responsável: Equipe técnica da Diretoria de TI.	
Entradas: Dados com informações do problema.	
Saídas: Inicia o processo de gerenciamento de Problema.	

5.8. Pré-Requisitos para Implantação

O Modelo de MGE, conforme as diretrizes estabelecidas pelo ITIL 4, requer o atendimento a um conjunto de pré-requisitos técnicos, processuais e organizacionais indispensáveis à sua efetividade no contexto institucional. A implantação dos fluxos de MGE, sejam automatizados ou manuais, depende diretamente da integração entre sistemas e ferramentas, da padronização de procedimentos, da confiabilidade das informações e do grau de maturidade em governança de TIC.

Entre os mecanismos essenciais para a efetividade do modelo, destacam-se a necessidade de manter um inventário atualizado dos ativos ou itens de configuração (IC), a definição clara de papéis e responsabilidades e a adoção de ferramentas apropriadas para coleta e análise de dados, mesmo quando envolvam soluções de baixo custo ou recursos limitados. Essas práticas encontram respaldo nas recomendações da ITIL 4, que enfatizam a importância da visibilidade contínua sobre os serviços de TI e a capacidade de resposta proativa diante de alterações no estado operacional [1].

Para contornar restrições orçamentárias e acelerar a implantação do MGE, recomenda-se a adoção de ferramentas *open source* (ex: Zabbix, Prometheus e GLPI). que dispensam custos de licenciamento, minimizam a dependência de fornecedores e oferecem elevado potencial de customização local. Estudos sobre adoção organizacional de software livre indicam que esses benefícios estratégicos são particularmente relevantes em ambientes públicos sujeitos a limitações de orçamento e a demandas por transparência tecnológica [92]

Os elementos fundamentais necessários para garantir a operação automatizada do fluxo MGE automático completo (1.0 a 1.22) estão sintetizados na Tabela 8, a qual apresenta os requisitos desejáveis para a execução plena do modelo:

Tabela 8 - Pré-Requisitos Desejáveis do Fluxo MGE Automático (1.0 a 1.22)

ID	Descrição
01	Sistema de monitoramento automatizado, capaz de coletar métricas, *logs* e eventos em tempo real (ex.: Zabbix, Nagios, Prometheus).
02	Integração via API ou *webhook* entre ferramenta de monitoramento e sistema de classificação/gestão de incidentes (ex.: Python REST, GLPI API).
03	Motor de decisão automatizado (ex.: lógica Fuzzy implementada em Python), capaz de classificar eventos com base em criticidade, impacto e urgência.

04	Sistema de ITSM (ex.: GLPI) configurado para abertura automática de chamados, categorização, escalonamento e registro de histórico.
05	Base de dados de inventário e configuração dos ativos monitorados, integrada ao sistema de monitoramento.
06	Definição formal de papéis e responsabilidades (ex: equipes de monitoração, gestores de incidente, com matriz RACI documentada).
07	Procedimentos operacionais documentados para cada etapa do fluxo automatizado (do disparo do evento à resolução e encerramento).
08	Canal de auditoria e rastreabilidade automatizada das ações, decisões e eventos, integrado ao sistema de ITSM e monitoramento.
09	Base de conhecimento institucional para registro de lições aprendidas, soluções aplicadas e informações para consulta das equipes.
10	Ambiente de testes e homologação para validação de integrações e automações antes da produção.

No caso do fluxo manual de monitoramento com geração de alerta (2.1 a 2.5), o atendimento a pré-requisitos de menor complexidade tecnológica é suficiente para assegurar rastreabilidade e padronização mínima das ações. A Tabela 9, consolida esses requisitos desejáveis, contemplando desde a manutenção de inventário básico de ativos até a formalização simplificada de registros de eventos e responsabilidades, permitindo que instituições com infraestrutura limitada executem o processo de forma controlada e progressivamente evoluam para níveis mais elevados de automação.

Tabela 9 – Pré-Requisitos do Fluxo de Start Manual (2.1 a 2.5)

ID	Descrição
01	Base de dados contendo identificação, localização, criticidade, dependências e responsáveis por cada ativo monitorado.
02	Documento técnico que define os ativos a serem monitorados, critérios de evento, métricas, níveis de severidade e periodicidade de análise.
03	Ferramentas operacionais (ex.: Zabbix, GLPI ou equivalentes) para coleta, visualização e análise de logs, métricas e dados históricos.
04	Designação formal das funções envolvidas no processo (quem inicia, quem coleta, quem analisa, quem classifica), por exemplo (Matriz RACI ou equivalente).
05	Procedimento Operacional Padrão (POP) que instrui a equipe sobre cada etapa do processo, garantindo padronização e reprodutibilidade.
06	Sistema ou ferramenta que permite o registro do evento, com histórico completo das ações executadas e decisões tomadas (ex.: GLPI, planilha controlada ou equivalente).

A execução eficaz do fluxo de Gerenciamento do Plano de Monitoração de Eventos depende da existência de condições institucionais, processuais e documentais que assegurem regularidade, rastreabilidade e transparência em todas as revisões realizadas. Esses elementos são fundamentais para manter a coerência entre o Plano de Monitoração e a política de governança de TI, permitindo que o processo evolua continuamente e se mantenha adequado às mudanças organizacionais e tecnológicas.

De acordo com os princípios do ITIL 4, as organizações devem estabelecer mecanismos de melhoria contínua capazes de garantir que suas práticas e serviços permaneçam alinhados às necessidades do negócio e aos objetivos estratégicos. O framework orienta que os processos de governança e gestão sejam monitorados e aperfeiçoados de forma constante, a fim de maximizar a criação de valor e manter a conformidade com os direcionamentos institucionais [1].

Além disso, o ITIL 4 reforça a necessidade de controle e registro sistemático das alterações nos serviços e processos, assegurando que cada modificação seja devidamente avaliada, autorizada e documentada. Esse controle rigoroso é essencial para preservar a integridade operacional, facilitar auditorias e garantir a rastreabilidade das decisões, elementos indispensáveis à governança de TIC.

Em contextos organizacionais com níveis iniciais de maturidade, o framework reconhece que a implementação desses requisitos pode ocorrer de forma gradual e evolutiva. Nesses casos, são aceitáveis soluções transitórias, como fluxos simplificados ou planilhas estruturadas, desde que estejam inseridas em um plano de aprimoramento contínuo, voltado ao fortalecimento dos controles e à consolidação das práticas de monitoramento.

Dessa forma, o cumprimento progressivo dos pré-requisitos técnicos, administrativos e documentais constitui um instrumento estratégico de governança, promovendo a sustentabilidade do processo de monitoramento de eventos e garantindo que ele continue a gerar valor, de maneira controlada e transparente, ao longo do tempo.

A seguir, a Tabela 10, apresenta os principais pré-requisitos necessários para a execução do fluxo de Gerenciamento do Plano de Monitoração:

Tabela 10 - Pré-Requisitos do Fluxo de Gerenciamento do Plano de Monitoração

ID	Descrição
01	Política formal de Governança de TIC, estabelecendo diretrizes, periodicidade e responsabilidades para a revisão e manutenção do Plano de Monitoração de Eventos, em conformidade com o modelo de governança institucional.
02	Relatórios consolidados de eventos e desempenho operacional, contendo dados históricos, indicadores de tendência, incidentes, exceções e resultados de ações corretivas, utilizados como insumo para a melhoria contínua.
03	Plano de Monitoração de Eventos vigente, devidamente documentado, controlado por versão e acessível às partes interessadas, com registro de atualizações e histórico de alterações.
04	Metodologia estruturada de análise crítica e melhoria contínua, com critérios definidos para identificação de não conformidades, oportunidades de aprimoramento e elaboração de planos de ação corretiva e preventiva.
05	Processo formal de validação e aprovação de alterações, com definição explícita de papéis, responsabilidades e critérios de decisão, apoiado por instrumentos como a Matriz RACI ou equivalente.
06	Ferramenta ou sistema de gestão documental que assegure versionamento, controle de acesso, rastreabilidade e comunicação das atualizações do Plano de Monitoração a todos os públicos relevantes.
07	Registro histórico de revisões e alterações, com identificação de data, responsável, descrição da mudança e justificativa, garantindo transparência e auditabilidade do processo de atualização.

O fluxo Monitorar, representa o ponto inicial da execução operacional da MGE, sendo responsável por transformar dados coletados sobre desempenho, disponibilidade e integridade dos ativos de TI em informações relevantes para a tomada de decisão na gestão de serviços. De acordo com os princípios da ITIL 4, a atividade de monitoração tem como finalidade assegurar a observação contínua do estado dos componentes de infraestrutura e dos serviços de TI, de modo a possibilitar a identificação proativa de desvios e o tratamento preventivo de falhas potenciais antes que impactem os usuários.

A Tabela 11, apresentada na sequência, sintetiza os pré-requisitos necessários ao correto funcionamento do fluxo, bem como alternativas operacionais adequadas a diferentes níveis de maturidade e disponibilidade de recursos.

Tabela 11 - Pré-Requisitos do Fluxo Monitorar

ID	Descrição
01	Existência de um Plano de Monitoração aprovado pela governança de TI e alinhado ao catálogo de serviços, contendo objetivos, escopo, periodicidade e critérios de escalonamento.
02	Disponibilidade de dados atualizados de inventário dos ativos monitorados, integrados à CMDB ou a uma base de configuração equivalente, para correlação precisa entre eventos e componentes.
03	Matriz de responsabilidades (RACI) definida, especificando papéis de operação, análise e escalonamento de eventos.
04	Definição formal de indicadores de desempenho (KPIs) e de seus respectivos limiares operacionais, derivados dos Acordos de Nível de Serviço (ANS) vigentes.
05	Implantação de ferramentas de coleta e agentes de monitoramento configurados para captura contínua de métricas e logs de desempenho e disponibilidade.
06	Estabelecimento de integração técnica entre as ferramentas de monitoração e o sistema ITSM, assegurando o registro automático e rastreável dos eventos detectados.
07	Elaboração e manutenção de POPs que orientem as atividades de monitoração, categorização e correlação de eventos.
08	Execução de programas de capacitação técnica para as equipes responsáveis pela operação e análise dos eventos, com atualização contínua conforme evolução das ferramentas.
09	Definição de canais formais de comunicação e escalonamento, parametrizados conforme as categorias de evento e níveis de serviço definidos nos ANS.

O fluxo MGE (5.0 a 5.6), apenas eventos de exceções, constitui uma versão simplificada e direcionada do processo principal da MGE (1.0 a 1.22). Sua estrutura deriva diretamente do modelo completo, mas contempla exclusivamente as etapas relacionadas ao tratamento de eventos classificados como exceção, suprimindo as fases de correlação, categorização e priorização que caracterizam o ciclo integral.

Essa configuração foi concebida para atender instituições em estágios iniciais de maturidade em governança e gestão de serviços de TIC ou que optem por implementar a prática de forma gradual, iniciando pela gestão de incidentes críticos e de alto impacto operacional. Ao limitar o escopo às exceções, o modelo viabiliza uma adoção controlada e incremental, permitindo à organização consolidar práticas de monitoramento, resposta e registro, sem comprometer a coerência com os princípios estruturantes da ITIL 4. Essa abordagem favorece a criação de um ambiente de aprendizado organizacional contínuo, que pode posteriormente evoluir até o modelo automatizado completo.

Para a operacionalização desse fluxo, torna-se indispensável o atendimento a um conjunto de pré-requisitos institucionais, processuais e tecnológicos, que asseguram a rastreabilidade, a padronização e a integridade das ações executadas. Esses elementos estabelecem as condições necessárias para que o tratamento de exceções ocorra de forma estruturada e eficiente, garantindo a confiabilidade dos registros e a efetividade das respostas às ocorrências críticas. A Tabela 12, a seguir, apresenta esses pré-requisitos, ajustados ao escopo simplificado do fluxo MGE (5.0 a 5.6).

Tabela 12 - Pré-Requisitos do Fluxo Monitorar

ID	Descrição
01	Documento institucional que formalize a adoção do modelo simplificado de Monitoração e Gerenciamento de Eventos, aplicável exclusivamente a incidentes classificados como exceção.
02	Política de Governança de TIC que defina critérios para priorização e tratamento de eventos críticos e de alto impacto operacional.
03	Base de dados atualizada contendo os ativos monitorados, responsáveis e relações de dependência entre serviços essenciais.
04	Ferramenta de monitoramento (ex.: Zabbix) configurada para identificar automaticamente eventos classificados como exceção, sem intervenção manual.
05	POP descrevendo as etapas de análise, definição de ação, autorização e execução de medidas corretivas.
06	Registro histórico de eventos e incidentes críticos para subsidiar ações corretivas e análise de recorrência.
07	Mecanismo de controle e aprovação formal para ações que exijam autorização superior, com registro das decisões tomadas.
08	Plano de Ação e contingência contendo alternativas de execução e procedimentos de solução de contorno.
09	Base de Conhecimento institucional com registros de violações, soluções adotadas e lições aprendidas.
10	Canal de comunicação definido para informar as partes interessadas sobre a execução de ações corretivas e o restabelecimento dos serviços.

5.9. Matriz RACI

No que se refere à definição de responsabilidades e papéis nos processos automatizados, destaca-se a necessidade de instrumentos formais de gestão que garantam clareza na atribuição de tarefas, níveis de autoridade e responsabilidades em cada etapa do fluxo. Nesse sentido, a matriz *Responsible, Accountable, Consulted, Informed* (RACI) constitui

uma ferramenta amplamente reconhecida para o mapeamento e a documentação das responsabilidades organizacionais.

De acordo com [93], a matriz RACI contribui para a definição dos responsáveis diretos (*Responsible*), das autoridades aprovadoras (*Accountable*), dos profissionais consultados (*Consulted*) e dos destinatários de informação (*Informed*), permitindo descrever de forma estruturada as funções, responsabilidades e níveis de autoridade vinculados a cada atividade. Além disso, a aplicação da RACI serve de base para o plano de comunicação do processo, especificando quem deve ser informado, em que momento e com qual nível de detalhamento.

A relevância da definição formal de papéis e responsabilidades na governança de TI é evidenciada por [94], que demonstram que a efetividade do ITIL como modelo de referência para governança depende, entre outros fatores, da existência de processos padronizados e controlados, com responsabilidades claramente atribuídas e propriedade de processo bem definida. Esses achados reforçam o princípio central que sustenta a aplicação da matriz RACI, a necessidade de clareza organizacional e responsabilidades nas atividades de TIC.

Sua adoção é amplamente recomendada pelos principais frameworks de governança e gestão de serviços de TI, incluindo o ITIL, cuja aplicação prática é exemplificada por [55]. Os autores demonstram que o uso da matriz RACI em processos de gerenciamento de incidentes, conforme as diretrizes do ITIL, promove a definição clara de papéis e responsabilidades, reduz falhas de comunicação e aumenta a eficiência operacional das equipes de suporte.

5.10. Avaliação por Especialistas do Fluxo MGE

A avaliação diagnóstica do modelo proposto teve como objetivo coletar a percepção crítica de especialistas com ampla experiência em TIC. Para tanto, foi disponibilizada aos profissionais, em ambiente controlado, a documentação completa dos fluxos modelados em notação BPMN de alta resolução, permitindo análise detalhada e feedbacks fundamentados, em alinhamento às recomendações metodológicas de [95].

O processo de coleta de dados foi realizado por meio da plataforma *Google Forms*, no período de 30 de outubro a 07 de novembro de 2023, totalizando 17 respostas válidas. As questões iniciais P.1 a P.3, buscaram caracterizar o perfil dos participantes, conforme Tabela 13.

Tabela 13 – Questões de Qualificação dos Respondentes

Questão	Descrição da pergunta
P.1.	Você se enquadra em qual categoria?
P.2.	Há quanto tempo você está envolvido no gerenciamento, tomada de decisões, especificação de projetos e/ou manutenção da infraestrutura de TI?
P.3.	De acordo com sua experiência você se classifica como

O grupo de respondentes distribui-se entre os seguintes cargos: Diretor ou Gestor de TI (3), Gerente de TI ou de Infraestrutura de TI (6), Analista de TI, Analista de Projetos ou Coordenador de TI (5) e Consultor de TI ou Técnico de Infraestrutura de TI (3). A primeira questão do instrumento (P.1) foi dedicada à identificação da qualificação profissional dos participantes, permitindo evidenciar a diversidade de funções e responsabilidades presentes entre os especialistas em TIC, conforme ilustrado na Figura 7.

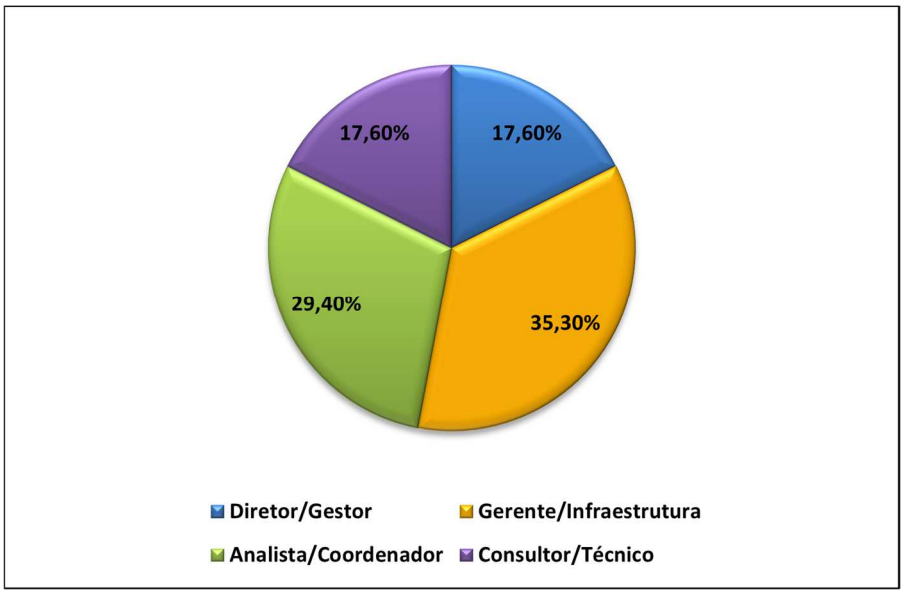


Figura 7 - Percentual dos cargos ocupados pelos respondentes. Fonte: Autor.

O resultado da segunda questão (P.2), Figura 8, é dedicada a aferir o tempo de atuação em TIC dos respondentes, revelou predominância de profissionais com mais de oito anos de experiência (12). Em seguida, os participantes com um a quatro anos (4) e aqueles com

seis a oito anos (1). Nenhum especialista declarou tempo de atuação entre quatro e seis anos (0).

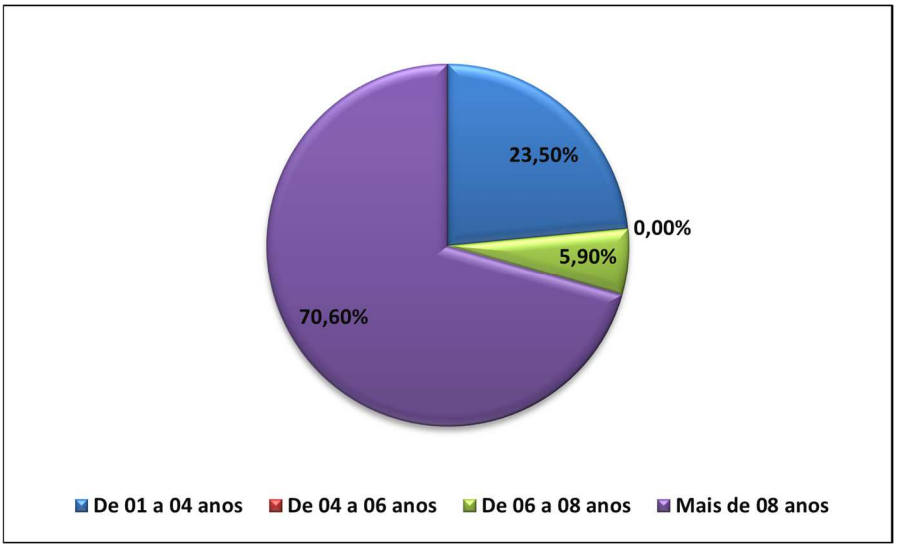


Figura 8 - Tempo de atuação dos respondentes. Fonte: Autor.

A terceira questão (P.3) investigou o grau de experiência profissional dos participantes. Entre os 17 respondentes, 9 declararam-se “Especialistas”, 5 posicionaram-se no nível “Sênior”, 3 enquadraram-se como “Pleno” e nenhum se identificou como “Júnior”. Esses dados evidenciam a predominância de profissionais altamente experientes, o que reforça a robustez das contribuições fornecidas para a avaliação do modelo, conforme gráfico ilustrado na Figura 9.

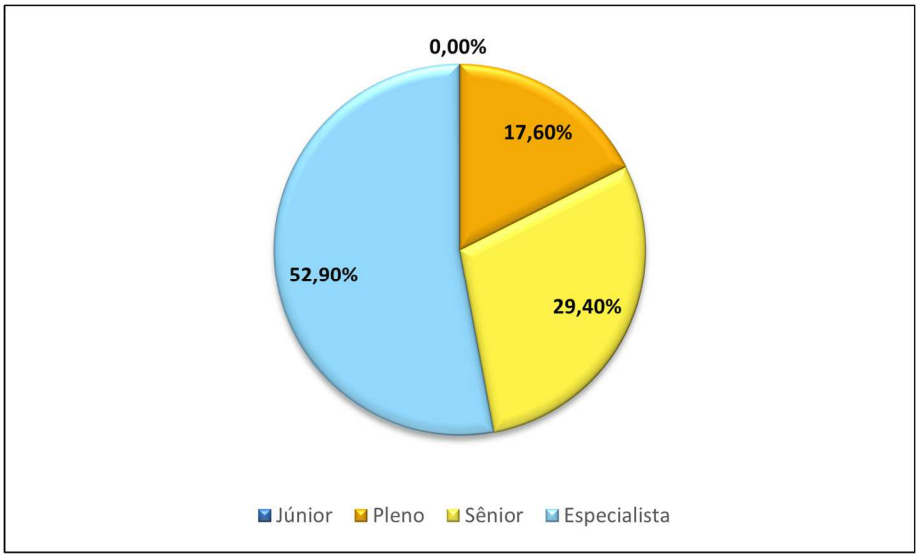


Figura 9 - Grau de experiência dos respondentes. Fonte: Autor.

Após a coleta dos dados relativos as perguntas P.1 a P.3, os respondentes receberam previamente materiais explicativos, incluindo os diagramas dos fluxos de atividades modelados em BPMN, Figuras 1, 3 a 6, um documento detalhando cada etapa do modelo e tabelas com informações sobre os processos, como objetivos, responsáveis, entradas, saídas e descrições.

A pesquisa foi composta por 6 questões, das 5 cinco empregaram a Escala de *Likert* de 1 a 5 pontos, variando de "discordo totalmente" a "concordo totalmente", conforme o instrumento original proposto por [96] e as diretrizes de refinamento metodológico de [97]. Essa estrutura quantitativa possibilitou mensurar a adequação do modelo sugerido, enquanto uma questão de formato aberto capturou percepções qualitativas, resultando em uma avaliação abrangente e robusta do processo proposto.

A Tabela 14, exibe as questões apresentadas aos respondentes para análise e avaliação do modelo proposto.

Tabela 14 – Questões de Avaliação do Modelo Proposto

Questão	Descrição da pergunta
P.1.	O modelo proposto de Gerenciamento de Monitoração e Evento segue um fluxo lógico de execução e está em consonância com as melhores práticas de gestão como o ITIL 4?
P.2.	Como você avalia a eficácia do Modelo de Monitoração e Eventos com base no ITIL 4 em termos de identificação proativa de incidentes, resposta oportuna e minimização de impacto nos serviços de TI?
P.3.	Na sua opinião, quão bem o Modelo proposto se adapta às mudanças nas necessidades de TI e aos avanços tecnológicos, assegurando que permaneça alinhado com as melhores práticas e inovações do setor?
P.4.	Como você avalia a eficácia da interação e trabalho conjunto das equipes no fluxo de Monitoração e Eventos, no que se refere à troca de informações, coordenação e resolução eficiente de incidentes?
P.5.	Você considera que o processo sugerido pode ser plenamente adotado ou trazer contribuições valiosas para a atual Gestão de Monitoramento em sua organização?
P.6.	Dê sua sugestão sobre o modelo proposto:

Os resultados obtidos demonstraram níveis satisfatórios entre os especialistas em relação ao modelo proposto. A questão P.1 obteve média de 4,29, indicando percepção favorável quanto à clareza da qualificação profissional considerada; P.2 registrou média de

4,58, evidenciando aprovação expressiva do tempo de atuação contemplado; P.3 alcançou média de 4,52, confirmando a adequação do grau de experiência exigido; P.4 apresentou média de 4,47, demonstrando boa aceitação dos processos e fluxos modelados; e P.5 despontou com a média mais alta, 4,88, reforçando a robustez geral e a relevância prática do modelo de monitoramento e gerenciamento de eventos.

A sexta questão P.6, foi estruturada em formato aberto, com o intuito de captar percepções qualitativas que complementassem a avaliação numérica obtida nas perguntas baseadas na Escala de Likert. As 17 respostas textuais foram analisadas por meio de codificação temática, resultando em três categorias de síntese—Relevância e alinhamento, Clareza e aplicabilidade e Valor público e visão sistêmica—cujos principais contributos e exemplos representativos estão consolidados na Tabela 15.

Tabela 15 – Principais Percepções P.6.

Categoria	Síntese das Contribuições	Exemplos de Respostas
Relevância e alinhamento	Reconhecimento do alinhamento do modelo com as melhores práticas da ITIL 4 e sua adequação à gestão pública de TI.	"O modelo proposto fornece uma base sólida para a gestão de serviços de TI." "O fluxo está bem alinhado com a ITIL 4."
Clareza e aplicabilidade	Destaque para a clareza do fluxo, facilidade de entendimento e aplicabilidade prática na rotina das organizações públicas.	"O modelo contribui para o melhor gerenciamento de TI." "A estrutura proposta é clara e de fácil adoção."
Valor público e visão sistêmica	Ênfase no potencial do modelo para agregar valor público, promover eficiência e oferecer uma visão integrada dos processos de TI.	"Imprescindível para a busca de uma gestão eficaz de TI preocupada com a entrega de valor público." "Proporciona uma visão holística e adaptativa."

Os comentários evidenciaram um grau satisfatório de aderência do modelo às boas práticas da ITIL 4, clareza de fluxo e potencial para gerar valor público, ao mesmo tempo em que apontaram melhorias pontuais, como a documentação do gerenciamento de problemas, a inclusão de etapas de comunicação pós-solução e a proposição de indicadores de desempenho.

De modo geral, essas percepções reforçam a robustez do modelo proposto e oferecem subsídios objetivos para ajustes futuros, com evidências consistentes de sua relevância e aplicabilidade no contexto da gestão de serviços de TIC no setor público.

Embora o processo avaliativo tenha seguido procedimentos metodológicos consistentes, a amostra de especialistas consultada apresenta limitações quanto ao seu tamanho e à sua composição, o que restringe a abrangência das percepções registradas.

Os resultados refletem, portanto, a análise de um grupo específico de profissionais com experiência direta no contexto estudado, o que deve ser considerado na interpretação dos achados.

5.11. Avaliação do Nível de Maturidade Institucional

A avaliação do nível de maturidade institucional em governança de TIC foi realizada por meio do modelo GAIA[5], aplicado através da ferramenta *Smart City Paraná* [87], que estrutura os domínios, critérios e pesos necessários para mensurar o grau de padronização, rastreabilidade, governança e capacidade operacional da instituição.

O instrumento contempla dimensões estruturais e processuais relacionadas à gestão de TI, permitindo a produção de um diagnóstico quantitativo e qualitativo do estágio de maturidade pré-implantação.

A utilização de instrumentos estruturados, como o Questionário de Diagnóstico de Avaliação (QDA), é fundamental para transformar evidências qualitativas em métricas quantificáveis e, assim, aferir de forma sistemática o grau de maturidade da governança de TIC na organização.

Segundo [98], modelos de maturidade em Governança de TI oferecem uma estrutura objetiva para diagnosticar lacunas e orientar estratégias de evolução contínua, pois traduzem práticas dispersas em indicadores mensuráveis e comparáveis ao longo do tempo. A adoção de instrumentos padronizados, como questionários ponderados e escalas de avaliação, não apenas facilita a coleta sistemática dos dados, mas também reforça a confiabilidade do processo de medição elemento crucial para respaldar decisões de investimento e priorização de iniciativas de melhoria em ambientes públicos complexos.

De acordo com [85], a eficácia dos artefatos em contextos institucionais depende de sua capacidade de representar com precisão o ambiente em que são aplicados. Nesse contexto, o QDA atua como uma ferramenta para apoiar a análise diagnóstica, a priorização de melhorias e o alinhamento estratégico, promovendo decisões baseadas em evidências.

---

[5] Disponível em: https://gaia2.uel.br/

A avaliação diagnóstica foi realizada por meio do QDA, estruturado de acordo com o modelo proposto por [85] e operacionalizado pela plataforma digital [87], a qual possibilita a coleta, a tabulação e a análise automatizada dos dados obtidos.

O instrumento possui 25 questões distribuídas em 8 eixos temáticos alinhados às práticas recomendadas pelo ITIL 4, conforme ilustrado na Figura 10, com cada item atribuído um peso de 1 a 3, de acordo com seu grau de importância para a governança institucional. As respostas seguem uma escala ordinal com valores entre +3 (concordância total) e -3 (discordância total). O cálculo da maturidade institucional é realizado utilizando uma soma ponderada adaptada do modelo original [85], garantindo clareza e rastreabilidade na análise dos resultados.

Para tabular e interpretar as respostas, adotamos a metodologia descrita por [99], na qual cada alternativa no questionário representa um estágio de maturidade institucional. Os participantes selecionam a opção que melhor reflete a situação atual da organização, e cada resposta recebe uma pontuação ponderada dentro de seu respectivo eixo temático.

Figura 10 - Eixos de governança de TIC utilizados no QDA. Fonte: Autor.

O impacto de cada resposta é calculado multiplicando-se o fator multiplicativo (FM), que expressa o grau de maturidade indicado pela alternativa escolhida, pelo peso da questão, que varia de acordo com sua relevância para o eixo avaliado, sendo 1

representando influência indireta e 2 representando influência direta. Por exemplo, uma resposta com FM = +3 e peso 2 resulta em um impacto de 6 pontos (3 x 2). Todos os impactos relacionados ao mesmo eixo são somados, formando o índice de maturidade para esse domínio específico.

Assim, questões mais estratégicas têm um impacto mais significativo no resultado final. A porcentagem consolidada desta análise é apresentada na Tabela 16.

Tabela 16 - Resultados da avaliação de maturidade separados por eixo.

Eixos Principais	Analista de Redes	Gerente de Redes	Analista de Projetos	Analista Banco de Dados	Pontuação Geral
Processos e Procedimentos	16,30%	22,83%	5,07%	35,51%	19,93%
Resposta a Eventos e Melhoria Contínua	13,95%	21,32%	2,33%	32,56%	17,54%
Tecnologia e Ferramentas	18,89%	27,22%	6,67%	46,67%	24,86%
Governança e Estratégia	15,69%	21,08%	6,86%	40,2%	20,96%
Cultura Organizacional	15,83%	15,83%	5%	28,33%	16,25%
Pessoas e Treinamento	12,96%	16,67%	3,7%	25,93%	14,81%
Gestão de Informação e Dados	10,61%	18,18%	2,02%	39,39%	17,55%
Escalabilidade e Crescimento	8,85%	15,10%	2,08%	39,58%	16,4%

A Figura 11, apresenta os resultados em um gráfico de radar, usando uma paleta de cores adaptada para acessibilidade de acordo com as diretrizes de segurança para daltônicos [100]. Essa visualização permite a identificação das áreas que mais precisam de melhorias e apoia ações estratégicas direcionadas para a organização.

Com base nessa análise, a cada eixo é atribuído um nível de maturidade de gestão de acordo com a porcentagem obtida: ($0 \leq 20\%$) = nível 1; ($21\% \leq 40\%$) = nível 2; ($41\% \leq 60\%$) = nível 3; ($61\% \leq 80\%$) = nível 4 e ($81\% \leq 100\%$) = nível 5. Essa abordagem permite uma avaliação objetiva da maturidade da instituição para cada eixo.

Vale destacar que o questionário integral contendo as 25 questões, suas escalas de resposta e pesos atribuídos a cada eixo, está apresentado no Apêndice H, permitindo plena rastreabilidade dos dados utilizados na avaliação de maturidade institucional.

A interpretação consolidada dos resultados oferece uma visão abrangente do posicionamento institucional em cada eixo de análise, destacando pontos fortes e áreas que requerem desenvolvimento.

Esse panorama inicial estabelece um marco referencial para avaliações subsequentes e orienta a tomada de decisão estratégica, assegurando que futuras iniciativas de melhoria sejam alinhadas às reais necessidades organizacionais.

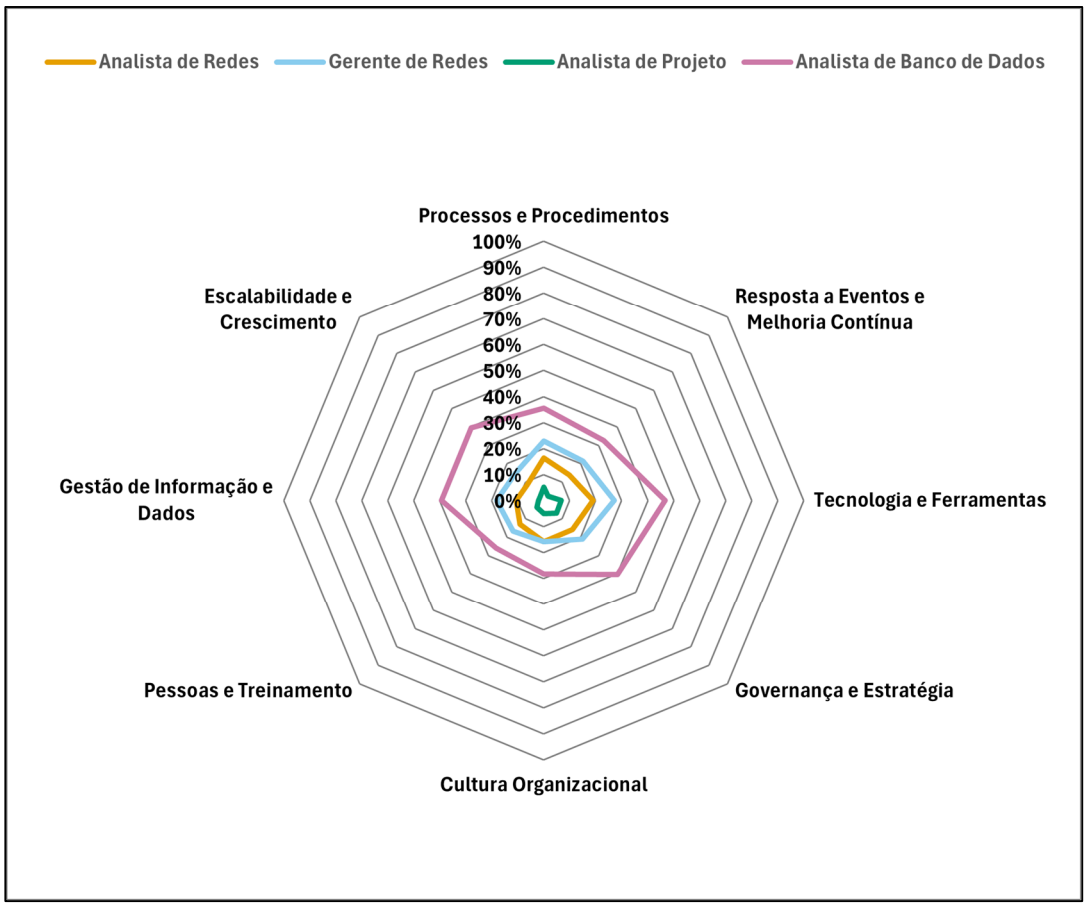


Figura 11 - Gráfico radar da maturidade institucional por eixos. Fonte: Autor.

Cabe destacar, que a avaliação do nível de maturidade institucional também apresenta limitações derivadas do caráter restrito do grupo de respondentes, composto por profissionais com conhecimento específico dos processos avaliados.

Embora esse recorte garanta maior precisão na análise, ele também reduz a possibilidade de captar percepções mais amplas sobre a organização. Assim, os resultados obtidos devem ser entendidos como representativos do ponto de vista desse grupo especializado, compondo uma linha de base inicial adequada ao propósito diagnóstico desta pesquisa.

5.12. Automação do Modelo Proposto

A automação do MGE foi concebida para proporcionar controle integral, escalável e auditável de todo o ciclo de incidentes e eventos. O modelo integra três módulos: Zabbix, MIF e GLPI, interligados por APIs *RESTful*. A arquitetura modular favorece a escalabilidade, simplifica a manutenção e permite futuras integrações. Diferenciando-se de abordagens reativas, o modelo estabelece monitoramento contínuo, classificação inteligente e resposta automatizada, promovendo decisões mais precisas e maior eficiência operacional. Para este cenário, utilizou-se Zabbix 7.4, MIF em Python sobre Ubuntu 24.04 LTS e GLPI 10.0.19.

5.13. Arquitetura Integrada do Sistema

O ciclo operacional inicia-se com a monitoração contínua dos ativos de TI pelo ZABBIX, responsável por identificar eventos relevantes, como falhas, alterações de estado ou degradação de desempenho.

A Figura 12, ilustra de forma geral como é feito a integração do sistema MGE automatizado.

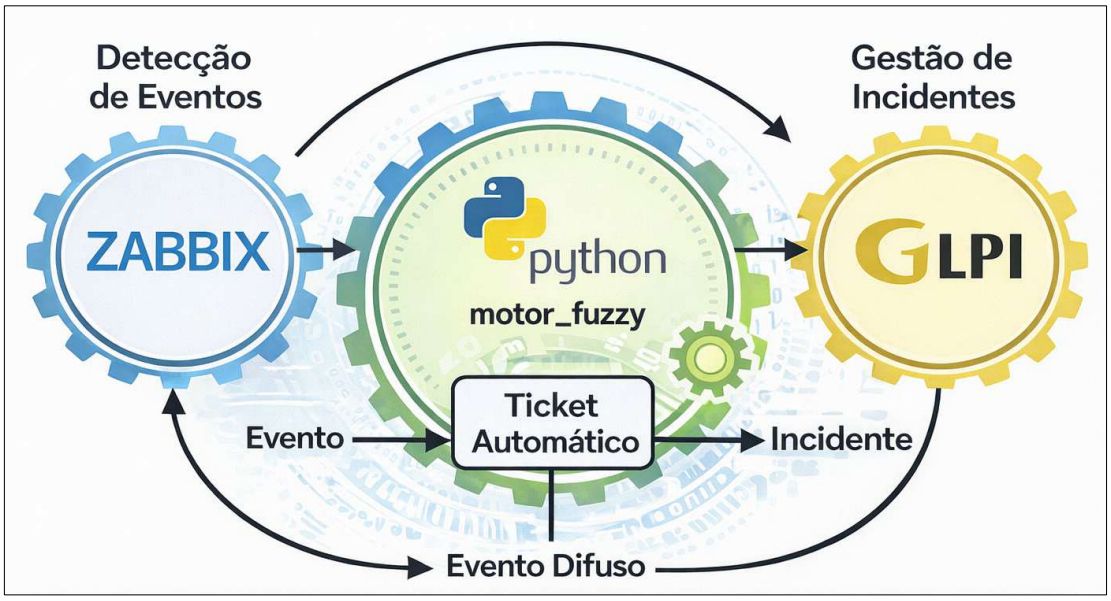


Figura 12 - Fluxo de operação entre ZABBIX, MIF e GLPI. Fonte: Autor.

Os eventos detectados são encaminhados automaticamente ao MIF por meio de requisições *HTTP POST*, utilizando *API REST* desenvolvida em Python, onde são

classificados quanto à criticidade por meio de uma matriz Fuzzy baseada nas variáveis impacto e urgência.

Após a classificação e a verificação de duplicidade (registro local do ID do evento), um novo *HTTP POST* é enviado à *API REST* do GLPI, que efetua a abertura automática do ticket, já categorizado conforme o nível de criticidade atribuído.

Toda a comunicação entre módulos ocorre exclusivamente por *APIs REST*, com *payloads JSON*, autenticação baseada em token e tráfego restrito à rede interna, garantindo confidencialidade e integridade dos dados.

5.14. Módulo de Monitoração: ZABBIX

A versatilidade da plataforma ZABBIX reside em sua arquitetura de coleta de dados híbrida. O sistema emprega tanto agentes de *software* nativos (*zabbix_agent*) para uma telemetria granular em nível de *host*, quanto mecanismos de monitoramento sem agente (*agentless*) [101].

Essa segunda abordagem utiliza protocolos como *Simple Network Management Protocol* (SNMP) para ativos de rede, *Intelligent Platform Management Interface* (IPMI) para o gerenciamento de *hardware* e *Java Management Extensions* (JMX) para aplicações, garantindo, dessa forma, a monitoração integral e a coleta de telemetria abrangente em ecossistemas de software e infraestrutura com topologia diversificada [101].

A ferramenta atua como o ponto de entrada do modelo, sendo responsável pela coleta contínua de métricas e pela detecção de eventos em uma ampla gama de ativos, como servidores, dispositivos de rede, aplicações e bancos de dados [101].

A configuração é baseada no uso de *templates* e *triggers*, que definem as condições anômalas e os limiares para a identificação de eventos relevantes. Ao detectar um evento, é acionado a *trigger* correspondente, executando uma ação de notificação.

Nesta arquitetura, a ação invoca um script customizado via *webhook*, que extrai dados essenciais do evento e os envia ao MIF via *HTTP POST* (*JSON*), protegido por autenticação via *token*, mitigando riscos de interceptação.

A capacidade de integração nativa da solução via *API REST*, combinada com a flexibilidade dos *webhooks*, foi um fator determinante para sua escolha. Essas funcionalidades viabilizam um alto nível de automação e facilitam a adaptação dos fluxos de monitoramento às necessidades do *framework* [101].

5.15. Matriz Fuzzy Multicriterio 5x5

Para atribuir criticidade a eventos de TI, conforme a Figura 2, etapa (1.7 Aplicar Matriz e Criticidade), o modelo utiliza aplica a MFMC, estruturada em uma grade 5x5, que combina os níveis linguísticos de impacto e urgência, variando de (Muito Baixo a Muito Alto). Essa estrutura permite a geração de classificações graduais em cinco níveis operacionais, com base na lógica Fuzzy [102], [103]

Ao adotar princípios de decisão multicritério, a matriz permite ajustar os pesos atribuídos aos critérios avalia dos e incorporar variáveis contextuais relevantes, como o grau de redundância ou exposição a falhas, garantindo maior aderência à realidade organizacional [102], [42]

Além disso, os níveis de criticidade atribuídos pela MFMC são representados por meio de uma codificação visual inspirada no modelo de cores do semáforo (verde, amarelo, laranja, vermelho), conforme mostrado na Tabela 17, adaptada de [42].

Para garantir a acessibilidade para usuários com deficiência na visão de cores, a paleta foi adaptada de acordo com esquemas seguros para daltônicos, conforme recomendado por [100]. Essa padronização aprimora a comunicação visual e acelera a priorização das ações necessárias.

A interpretação operacional dessa codificação segue uma lógica gradual: eventos classificados como "Muito Baixo" exigem apenas monitoramento; "Baixo" envolve monitoramento de rotina ou medidas preventivas básicas; "Médio" requer ações programadas com prioridade moderada; "Alto" requer uma resposta imediata e possível escalonamento; e "Muito Alto" exige intervenção urgente com priorização máxima. Essa gradação esclarece as prioridades e orienta objetivamente as ações apropriadas a cada nível de criticidade.

O nível "Muito Alto" destaca a necessidade de resposta imediata e priorização máxima, exigindo intervenção urgente. A Matriz MFMC estabelece os critérios de impacto (eixo vertical) e urgência (eixo horizontal), permitindo uma análise integrada tanto da gravidade quanto da velocidade necessária para lidar com os eventos. Isso resulta em avaliações mais precisas e proporcionais [42], em linha com as diretrizes do ITIL 4, que enfatizam a importância da padronização e da eficiência na classificação e no tratamento de eventos de TI [1].

Além disso, o modelo segue os princípios recomendados por [18], que orientam o uso de métodos estruturados para monitoramento, avaliação e gerenciamento de riscos em processos de tecnologia, fortalecendo a governança e a tomada de decisões em ambientes institucionais complexos.

Para garantir a padronização e facilitar a visualização dos resultados, os níveis de criticidade são classificados usando as siglas MB (Muito Baixo), B (Baixo), M (Médio), A (Alto) e MA (Muito Alto). Na matriz, o eixo X representa o critério de impacto e o eixo Y corresponde à urgência. Essa convenção simplifica a leitura e a rápida interpretação dos resultados nas análises e aplicações operacionais do MFMC.

Tabela 17 - Níveis de criticidade: impacto (X) e urgência (Y). Adaptado de [42].

X \ Y	**Muito Baixo**	**Baixo**	**Médio**	**Alto**	**Muito Alto**
Muito Baixo	Muito Baixo	Baixo	Baixo	Médio	Médio
Baixo	Baixo	Baixo	Médio	Médio	Alto
Médio	Baixo	Médio	Médio	Alto	Alto
Alto	Médio	Médio	Alto	Alto	Muito Alto
Muito Alto	Médio	Alto	Alto	Muito Alto	Muito Alto

A Figura 13, mostra as curvas de relevância em forma de sino que representam a escala de criticidade da Matriz MFMC, baseada em valores de pertinência Fuzzy de 1 a 9, centrados em níveis linguísticos de "Muito Baixo" a "Muito Alto".

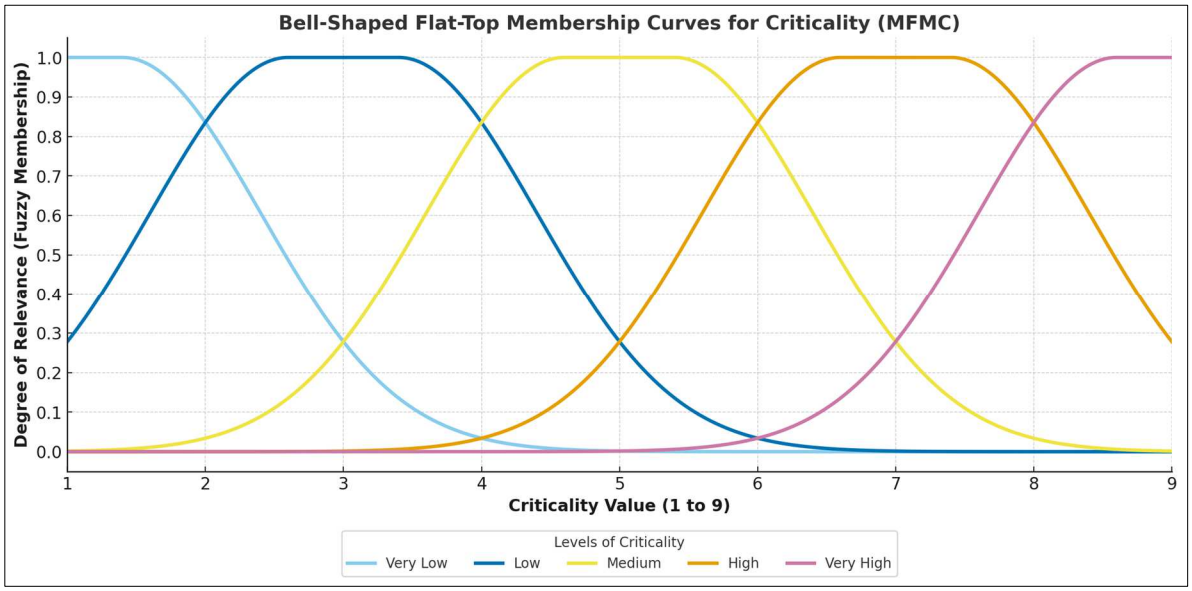


Figura 13 - Curvas bell-shaped x nível de criticidade. Adaptado de [102].

Este modelo permite transições suaves entre categorias de criticidade e maior precisão na avaliação de eventos limítrofes [104], seguindo as melhores práticas internacionais em gestão de risco multicritério [42] e apoiando avaliações mais realistas e adaptáveis.

A representação gráfica das curvas em forma de sino na Matriz MFMC mostra que cada nível de criticidade é modelado para permitir sobreposição e gradação entre categorias adjacentes, permitindo que eventos próximos aos limites entre dois níveis pertençam parcialmente a ambos [104].

Essa abordagem elimina a rigidez dos modelos binários e favorece avaliações mais realistas e adaptáveis da dinâmica dos eventos monitorados em TI, em linha com as diretrizes discutidas por [42].

Na Figura 13, o eixo horizontal (x) indica o nível de criticidade composto, variando de 1 a 9, resultante da combinação de impacto e urgência atribuídos pela Matriz MFMC. O eixo vertical (y), por sua vez, representa o grau de relevância Fuzzy de cada valor em relação aos cinco níveis linguísticos ("Muito Baixo" a "Muito Alto").

Essa representação nos permite identificar a afinidade de um evento com mais de um nível de criticidade, tornando a avaliação mais sensível e ajustada a situações de transição [42].

5.16. Arquitetura Operacional do Processo de Inferência Fuzzy

A lógica Fuzzy empregada na MFMC segue uma sequência metodológica bem estabelecida na literatura, estruturada em três fases complementares: (*i*) Fuzzificação, (*ii*) Inferência Fuzzy, e (*iii*) Defuzzificação, ilustrado na Figura 14.

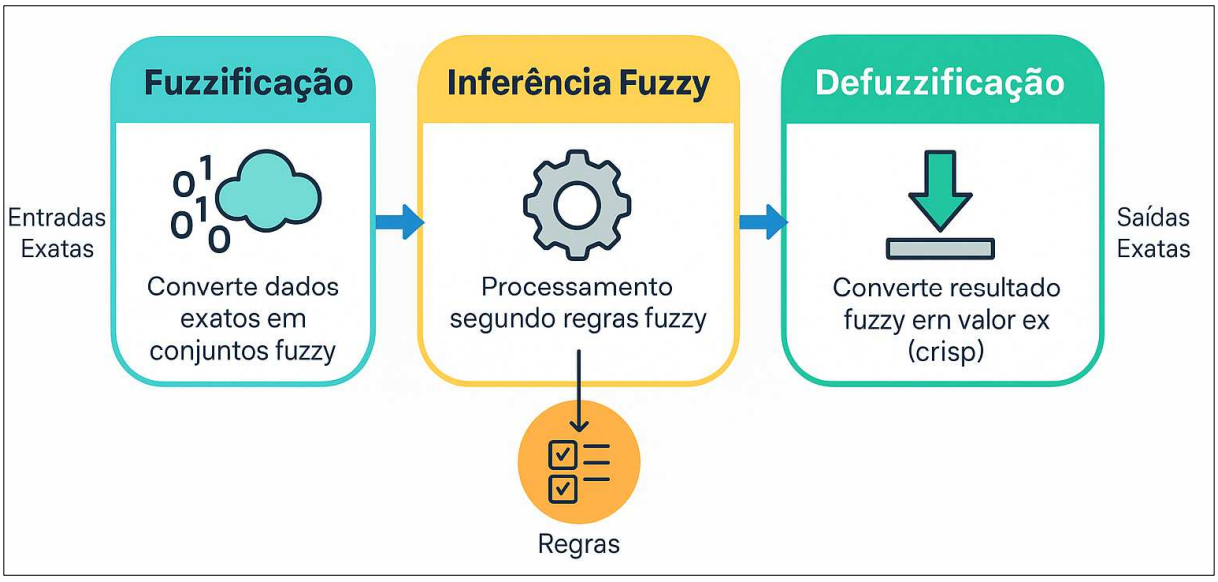


Figura 14 - Processo de Inferência Fuzzy. Adaptado de [3] .

Inicialmente, os valores numéricos de impacto e urgência são convertidos em graus de pertinência nas funções Fuzzy previamente definidas (Fuzzificação). Em seguida, aplica-se o mecanismo de inferência, pelo qual as regras do sistema são processadas e a equação correspondente é utilizada para determinar o nível de criticidade Fuzzy resultante.

Na sequência, realiza-se a defuzzificação, etapa responsável por transformar o resultado Fuzzy, representado por um conjunto de pertinências em um valor numérico *crisp* (valor obtido após a defuzzificação), que traduz de forma objetiva o nível de prioridade atribuído ao evento.

Esse encadeamento assegura coerência matemática, rastreabilidade das decisões e alinhamento com os fundamentos clássicos da teoria dos conjuntos Fuzzy.

5.17. Módulo de Classificação Inteligente: Motor Fuzzy

O Motor de Inferência Fuzzy (MIF) atua como *middleware* (intermediador) inteligente, integrando ZABBIX e GLPI e promovendo automação, contextualização e classificação avançada de eventos. Projetado como serviço *RESTful* assíncrono (*Flask*), o motor expõe *endpoint HTTP* para ingestão de eventos. Ao receber um evento via *webhook* (*HTTP POST, JSON*), realiza validação e normalização dos dados, assegurando integridade do *playload* e presença dos campos essenciais (*event_id, host_name e event*). *Playloads* inconsistentes são descartados e devidamente registrados em *log*, garantindo resiliência operacional.

Após a validação, o MIF executa o enriquecimento semântico do evento mediante consulta dinâmica a um arquivo de configuração (mapa_decisao.yaml). Esse arquivo define, de forma extensível e sem necessidade de alteração do código-fonte, o mapeamento entre *hosts*, tipos de eventos e parâmetros Fuzzy de impacto e urgência. Essa arquitetura configurável permite ajustes contínuos no modelo, viabilizando a inclusão de novos tipos de eventos e a calibração dos pesos utilizados na inferência Fuzzy, mantendo aderência ao comportamento real da infraestrutura monitorada.

Tal flexibilidade operacional permite que novas categorias de eventos ou alterações de pesos (parâmetros de pertinência Fuzzy) sejam configuradas diretamente pelo analista responsável, mantendo a aderência do modelo ao ambiente dinâmico da infraestrutura.

A Tabela 18, ilustra um exemplo de parametrização do arquivo (mapa_decisão.yaml) relacionando ativos x criticidade, baseado em impacto e urgência.

Tabela 18 – Exemplo do Mapa de Decisão: Criticidade x Ativo

Problema (switch)	Impacto	Urgência	Descrição
Dispositivo inacessível / Host inativo	5	5	Perda total do equipamento (afeta várias portas/segmentos).
Link inativo (uplink)	5	4	Segmento inteiro isolado; recuperação prioritária.
Perda de pacotes alta (>30%)	4	4	Degradação forte de serviços, usuários impactados.
Interface oscilante (uplink)	4	3	Instabilidade intermitente; risco de spanning-loop/perda.
Falha na fonte de alimentação (redundante)	2	2	Perda de redundância; risco de queda total ao falhar PSU restante.
Falha na ventoinha	4	3	Risco térmico crescente; pode evoluir para down.
Alta temperatura	2	4	Indicador térmico; ação rápida evita down.
Alto uso da CPU (sustentado >90%)	3	3	Queda de performance/gerenciamento; frequentemente degradante.
Link inativo no acesso (usuário)	3	2	Impacto localizado; tratativa não imediata (ver SLA).

A Figura 15, as etapas do fluxo foram associadas a uma paleta cromática padronizada para facilitar a leitura do diagrama e evidenciar a transição entre funções. O azul-claro identifica os pontos de coleta de dados e registro inicial de eventos; o verde-claro destaca a correlação de métricas e a detecção de padrões de ocorrência; o amarelo-claro sinaliza a classificação do tipo de evento; o laranja-claro representa a avaliação de criticidade com base no cálculo Fuzzy de “impacto x urgência”; e o roxo-claro marca as etapas de decisão e tratamento, incluindo abertura, atualização e encerramento de tickets no sistema de *service d*esk. Esse esquema de cores favorece a compreensão visual do processo e reforça sua rastreabilidade em auditorias e discussões técnicas.

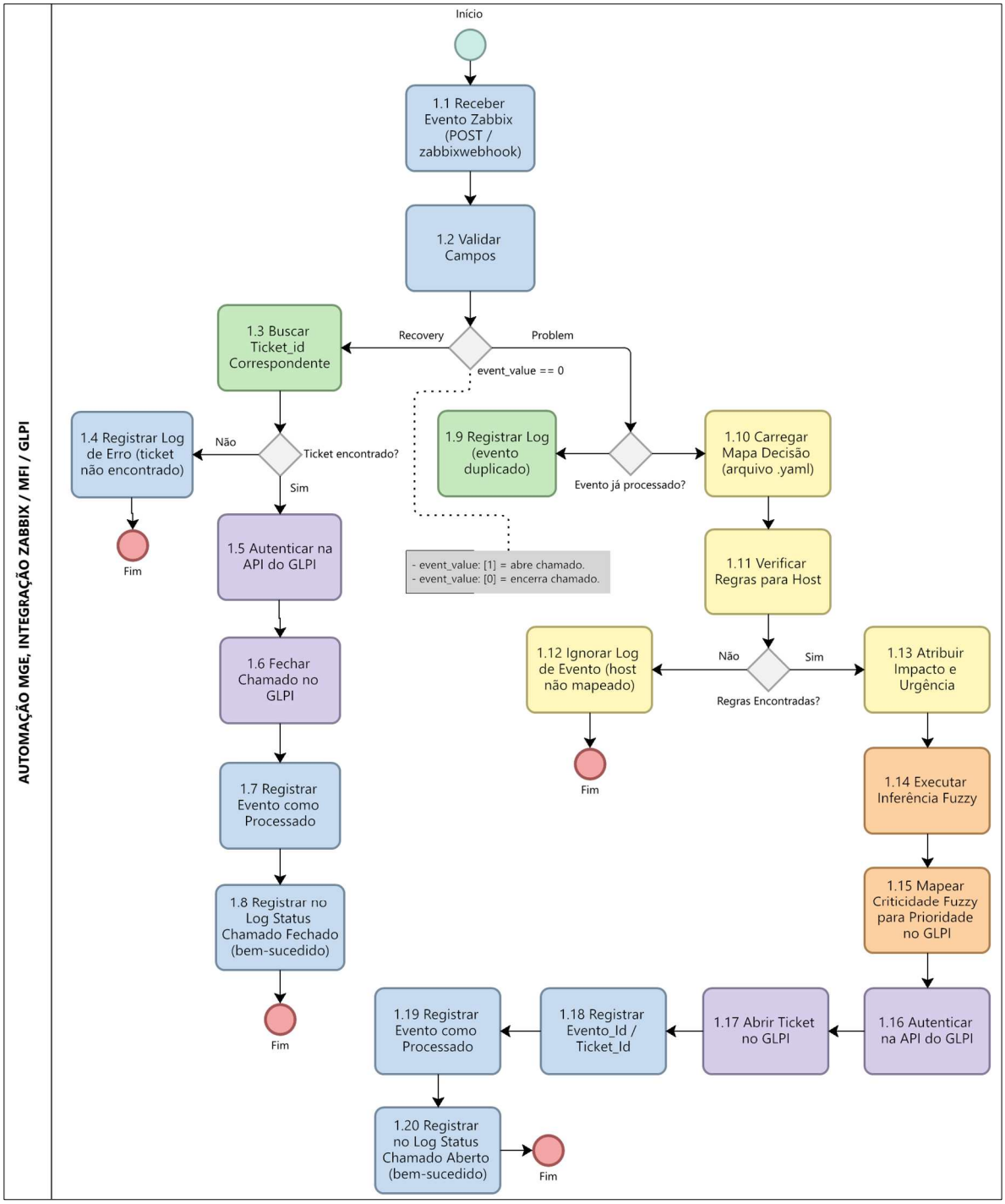


Figura 15 - Fluxo operacional do MIF. Legenda de cores: Azul claro = Coleta/registro; Verde claro = Correlação/controle; Amarelo claro = Classificação/regras; Laranja claro = Avaliação/priorização; Roxo claro = Registro no MIF e no ITSM. Fonte: Autor.

O núcleo do MIF é o mecanismo de inferência nebulosa descrito por [3]. Em vez de empregar limiares rígidos, a LF converte os valores numéricos de

impacto e urgência em variáveis linguísticas (por exemplo: Baixo, Médio ou Alto), utilizando funções de pertinência cujos graus variam, na prática, de 0 a 0,9, sendo 1 o limite teórico que representa pertinência máxima.

Com base nessas variáveis, o MIF aplica regras de inferência do tipo "[SE] Impacto = Alto (E) Urgência = Alta (ENTÃO) Criticidade = Muito Alta", um método que tem sido amplamente aplicado na priorização de eventos em ambientes de gestão de TIC [91], [40]. Em seguida, ele realiza a defuzzificação por centroide, reconhecido como o procedimento mais comum para obtenção de um valor numérico contínuo a partir de um conjunto Fuzzy [105]. Esse resultado é discretizado em níveis linguísticos (*Muito Baixa, Baixa, Média, Alta, Muito Alta*), que são mapeados para os campos de prioridade do GLPI.

O processo é totalmente transparente, com *logs* detalhados das variáveis de entrada, regras disparadas e saída final, garantindo a auditabilidade completa do processo decisório

A integração com o GLPI ocorre via *API REST* autenticada, e o MIF abre *tickets* automaticamente para cada evento classificado como crítico, padronizando o fluxo de trabalho, eliminando subjetividades e garantindo idempotência, isto é, o controle persistente dos eventos já processados que impede a criação de *tickets* duplicados. Embora o conceito esteja bem documentado na literatura de integração de sistemas [106], no presente trabalho ele foi aplicado de forma independente da FL, atuando especificamente na integração entre MIF e GLPI.

5.18. Módulo de Gestão de *Tickets*: GLPI

Nesta arquitetura, o software GLPI, versão 10.0.19, atua como *service desk* e ponto de rastreabilidade do ciclo de incidentes. A integração com o MIF ocorre via *API REST* autenticada por token, com *payloads JSON* trafegando em rede interna.

O MIF cria ou atualiza *tickets* por meio de requisições *HTTP*. Os campos mínimos registrados são: título, descrição contendo *host e event_id*, prioridade calculada pelo MIF, entidade ou categoria, grupo responsável e solicitante técnico. A prioridade resulta da criticidade defuzzificada (*defuzzification*) e é mapeada para níveis operacionais do GLPI (por exemplo, P5 a P1). O roteamento para o grupo responsável segue regras de mapeamento baseadas em host, tipo de evento ou serviço.

A idempotência é garantida pelo uso do *event_id* como chave de controle persistida pelo MIF e pela referência externa do ticket no GLPI. Retransmissões do mesmo evento promovem atualização do ticket existente, evitando duplicidades. Quando o ZABBIX sinaliza recuperação, o MIF altera o status do ticket para encerrado e registra anotação automática de fechamento.

A rastreabilidade é assegurada pelo histórico do GLPI e pelo log do MIF, que registram abertura, mudanças de prioridade, transferências entre grupos e encerramento, com carimbos de data e hora. Em falhas de comunicação ou validação, o MIF registra o erro, realiza novas tentativas com *backoff* e isola *payloads* inválidos para análise manual, preservando a consistência operacional sem interromper o processamento de outros eventos.

5.19. Monitoramento de Incidentes Automatizado em Execução

A sequência de Figuras a seguir ilustra o funcionamento integrado do modelo proposto, detalhando cada estágio do processo: (*i*) detecção de incidente (Zabbix), (*ii*) classificação de criticidade (MIF), e (*iii*) abertura de *ticket* (GLPI), em suas respectivas ferramentas.

A Figura 16, exibe a tela de incidentes do Zabbix, onde é possível visualizar o ativo (BORDA-02) com *status offline*. A interface apresenta detalhes do evento, incluindo carimbo de data/hora e evidencia a execução automática do *webhook* que entrega o *payload JSON* ao MIF.

O *log* da requisição *REST* confirma a transferência imediata desses dados para o MIF, onde o evento é classificado quanto à criticidade antes de desencadear a abertura do *ticket* no GLPI.

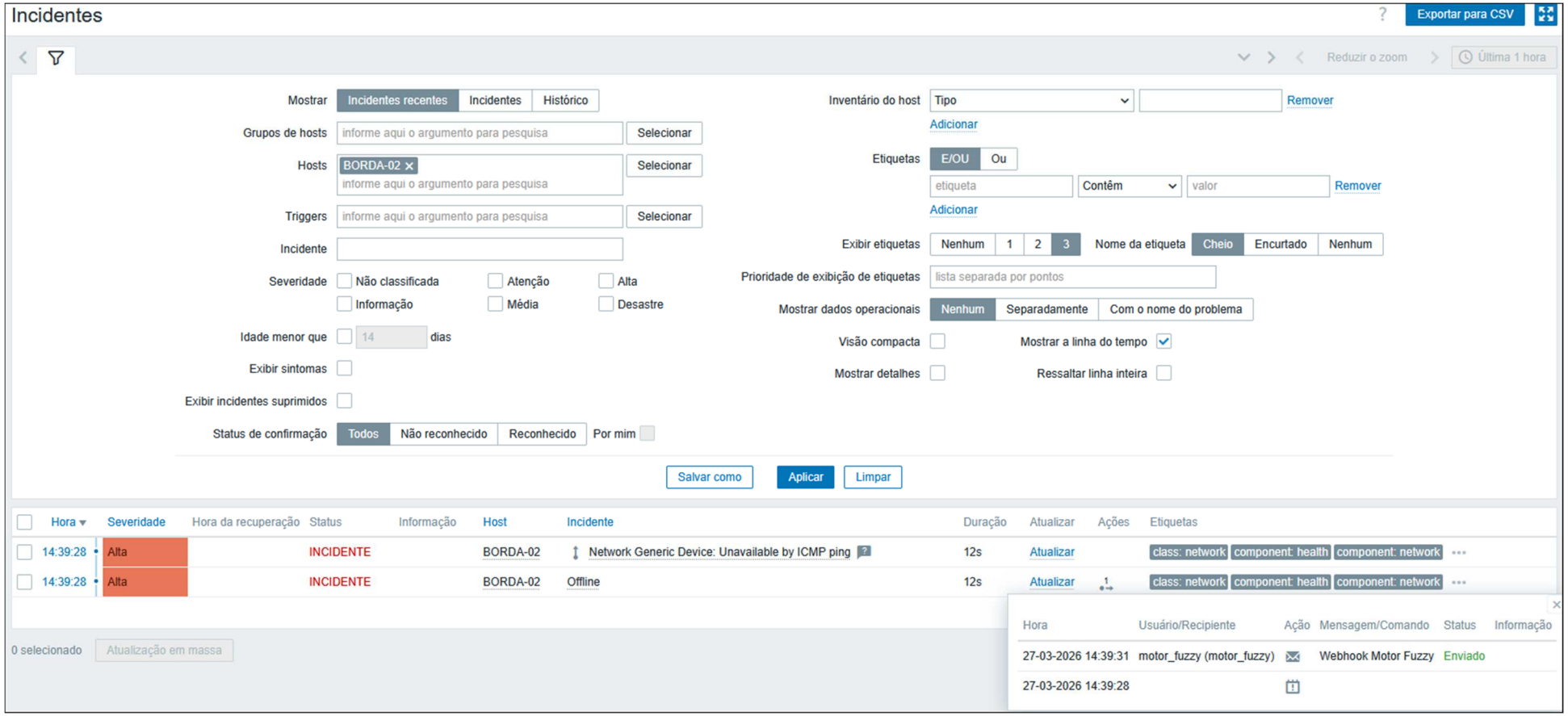


Figura 16 - Envio automatizado via *webhook* para o MIF. Fonte: Autor.

A Figura 17, exibe o log de operação do MIF em modo DEBUG, registrando o payload JSON recebido do Zabbix com os detalhes do evento e *trigger* correspondente.

A severidade informada pelo Zabbix é deliberadamente ignorada na classificação, pois o MIF aplica sua própria inferência Fuzzy, construída sobre um "mapa de decisão" que atribui graus de pertinência de impacto e urgência para cada tipo de ativo.

```
[DEBUG] Payload recebido: {'event_id': '291502', 'event_name':
'Offline', 'event_severity': 'High', 'event_value': '1',
'host_ip': '10.12.26.36', 'host_name': 'BORDA-02',
'trigger_id': '32625'}
[EVENTO] ID: 291502 | Host: BORDA-02 | Tipo: Offline | Im-
pacto: 3 | Urgência: 5 | Criticidade: 5.00 (Média)
[OK] Chamado aberto para event_id 291502. ticket_id: 41

[DEBUG] Payload recebido: {'event_id': '291502', 'event_na
me': 'Offline', 'event_severity': 'High', 'event_value': '0',
'host_ip': '10.12.26.33', 'host_name': 'BORDA-02', 'trigger
id': '32625'}
[OK] Chamado 41 fechado com sucesso para event_id 291502
```

Figura 17 - Controle de duplicidade para o incidente com ID 291502. Fonte: Autor.

Neste caso específico, o mapa define (impacto = 3 e urgência = 5) para o *host* (BORDA-02) quando o incidente for (*Offline*), contudo, esses valores são totalmente parametrizáveis, podendo ser ajustados a qualquer momento para refletir as necessidades e particularidades de cada instituição. Apenas esses dois parâmetros alimentam o cálculo, executado pelas 25 regras Fuzzy que, após a defuzzificação, resulta no valor 5,00 (Média) de criticidade.

O trecho do log também comprova o ciclo completo de gestão do incidente: primeiro a abertura automática do ticket (*ticket_id* 291502) e, em seguida, seu encerramento quando o MIF detecta a resolução do evento (*event_value* = 0).

A Figura 18, exibe o *ticket* no GLPI após o encerramento automático, documentando o ciclo completo do incidente. O MIF abre o *ticket* de forma automatizada, registrando nome do *host*, *eventID*, criticidade, data e hora de abertura. Ao detectar a resolução do evento no ZABBIX, o mesmo serviço realiza o fechamento. A imagem evidencia os carimbos de data/hora de abertura e encerramento, bem como uma entrada no histórico assinada pelo autor com a mensagem "Chamado fechado automaticamente pelo Motor Fuzzy". Embora não seja visível no histórico a entrada específica de abertura, os metadados do *ticket* comprovam a automação "ponta a ponta" e garantem a rastreabilidade do processo.

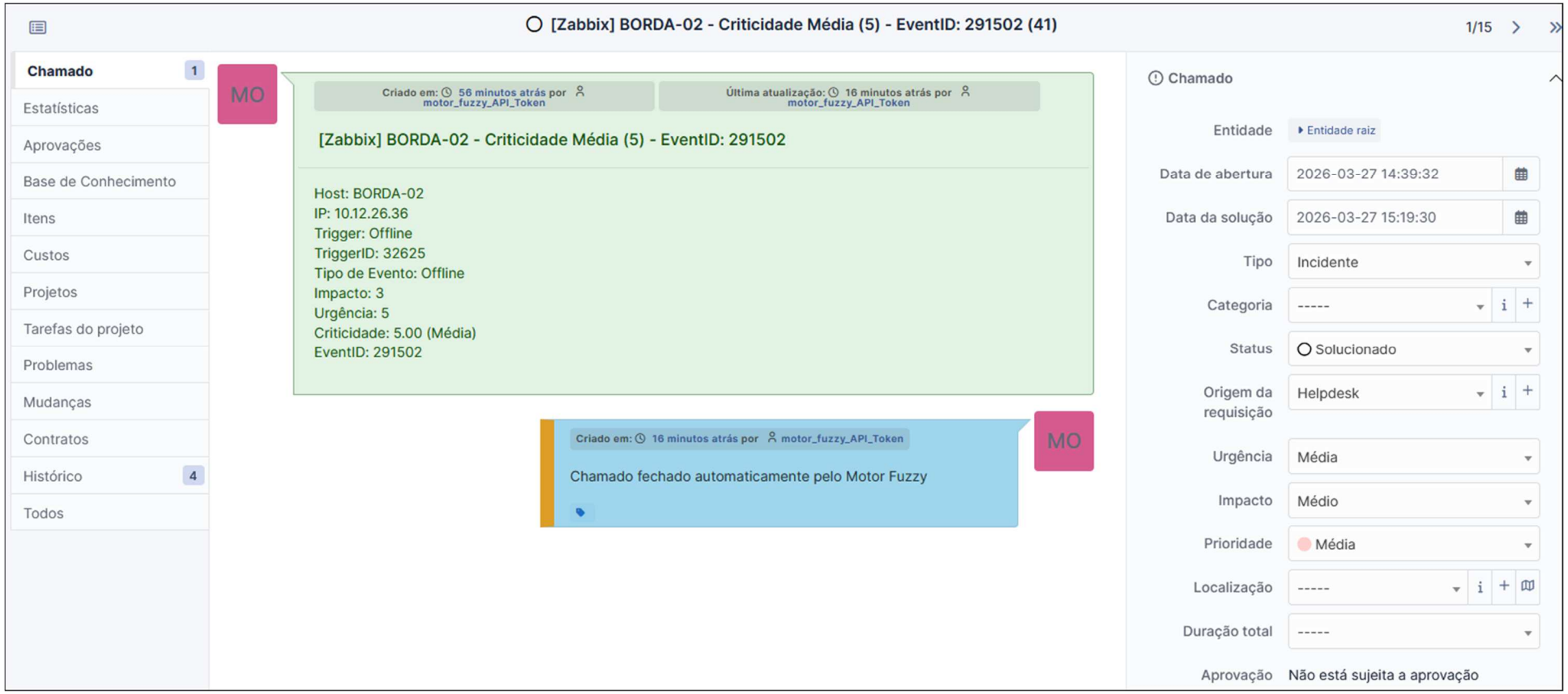


Figura 18 - *Ticket* encerrado automaticamente via MIF. Fonte: Autor.

5.20. Idempotência

A gestão automatizada de eventos em TIC exige mecanismos que atenúem oscilações intermitentes (*flapping*) e preservem a fidedignidade dos indicadores operacionais. No plano de monitoramento, o ZABBIX oferece a configuração de janelas de retenção (*hold-down timers*) nas *triggers*, assegurando que a transição de "problema" para "recuperação" só seja reconhecida quando a condição normal permanecer estável por um período mínimo previamente estabelecido (por exemplo, 10 minutos) [101].

Essa lógica posterga o encerramento lógico do incidente, evitando o ciclo vicioso de abertura e fechamento sucessivos de *tickets* gerados por oscilações rápidas. Ao suprimir falsos positivos, o mecanismo reforça a confiabilidade dos registros históricos e reduz o ruído operacional, fator crítico para ambientes de missão crítica que demandam alta disponibilidade.

Mesmo assim, há cenários em que múltiplos eventos equivalentes ainda chegam ao mecanismo de correlação. Para mitigar definitivamente a duplicidade de chamados, o MIF aplica uma lógica idempotente como segunda camada de controle, onde cada requisição recebida é confrontada com o conjunto de *tickets* abertos e caso um incidente similar já estiver em tratamento, o MIF apenas anexa a atualização, sem acionar nova abertura. Evidências de estudos mostram que juntar *tickets* iguais de forma inteligente torna o Service Desk mais eficiente e diminui a carga de trabalho da equipe [107], [80].

Essa arquitetura em camadas é corroborada por estudos de automação de *service desk* que demonstram ganhos substanciais de eficiência quando técnicas de consolidação e prevenção de duplicidade são combinadas a filtros de pré-processamento em tempo real. A integração do *hold-down timer* com a idempotência preserva a integridade dos dados nos painéis de gestão e direciona as equipes de suporte ao tratamento de ocorrências genuinamente distintas.

Por fim, o tempo adicional introduzido pela janela de retenção é incorporado ao cálculo do MTTR. Embora esse acréscimo eleve o valor do indicador, ele fornece representação mais fidedigna da experiência do usuário e do esforço necessário para garantir estabilidade operacional, justificando-se plenamente em contextos que priorizam confiabilidade sobre mera rapidez de encerramento [1].

Exemplo prático: Um switch sofre *flapping* e alterna várias vezes entre *off-line* e *on-line*, o ZABBIX, por meio da janela de retenção configurada na *trigger*, mantém o

estado de “problema” até que o *link* permaneça estável por “X tempo”, evitando abrir e fechar chamados a cada oscilação, em seguida, o MIF aplica sua lógica idempotente, confirmando se já existe *ticket* ativo para o mesmo evento antes de qualquer novo registro, assegurando uma dupla camada de proteção contra duplicidades.

A Figura 19, ilustra o mecanismo de idempotência do MIF: ao receber uma segunda notificação do (*event_id* 291502), o sistema detecta que o evento já foi tratado e devolve a resposta “Evento já processado!”, evitando *tickets* duplicados e mantendo o histórico consistente.

Figura 19 - Controle de duplicidade para o incidente com ID 291502. Fonte: Autor.

5.21. Métricas MTTD e MTTR: Sistema Legado

Para estabelecer um panorama longitudinal do desempenho operacional, foram extraídos 23.800 registros de incidentes do sistema legado, abrangendo todo o período de 2009 / 2025.

A triagem automática descartou 3.691 entradas (15,5 %) por inconsistências de preenchimento, das quais 62 não continham identificação de ano. Permaneceram 20.109 ocorrências válidas, consolidadas em planilha-síntese (.xlsx) gerada em 15 out. 2025, que servirá de repositório de referência para análises evolutivas.

A inspeção estatística completa confirma níveis elevados de latência operacional, especialmente na fase de resolução, refletindo a ausência de mecanismos de correlação automática e notificação em tempo real no fluxo manual vigente. Esses resultados

reforçam a motivação para implantar o modelo automatizado proposto, alinhado às melhores práticas da ITIL 4.

Para compor a linha de base que sustentará a avaliação do artefato, adotou-se o recorte dos últimos 90 dias imediatamente anteriores à implantação (15 jul. / 15 out. 2025). Nesse intervalo, foram consolidados 209 registros de incidentes, dos quais 160 foram considerados válidos para cálculo de MTTD e MTTR, após o descarte de 49 registros devido a inconsistências e incompletude dos dados, assegurando comparabilidade temporal sem comprometer a confiabilidade das métricas.

O processamento dos 160 registros válidos produziu um MTTD médio de 19,08 h e um MTTR médio de 4,92 dias, com desvios-padrão de 3,12 dias (MTTD) e 9,02 dias (MTTR), respectivamente. Tais valores evidenciam detecção predominantemente reativa e janelas prolongadas de reparo, características típicas de ambientes dependentes de registro manual.

A Figura 20, sintetiza os resultados, exibindo em um único painel as médias e os desvios-padrão de MTTD e MTTR referentes ao período avaliado. Essa visualização facilita a comparação entre as métricas e servirá, após a implantação do modelo automatizado, como referência para um novo levantamento, aplicado ao mesmo intervalo temporal, a fim de evidenciar os ganhos de desempenho obtidos com a automação.

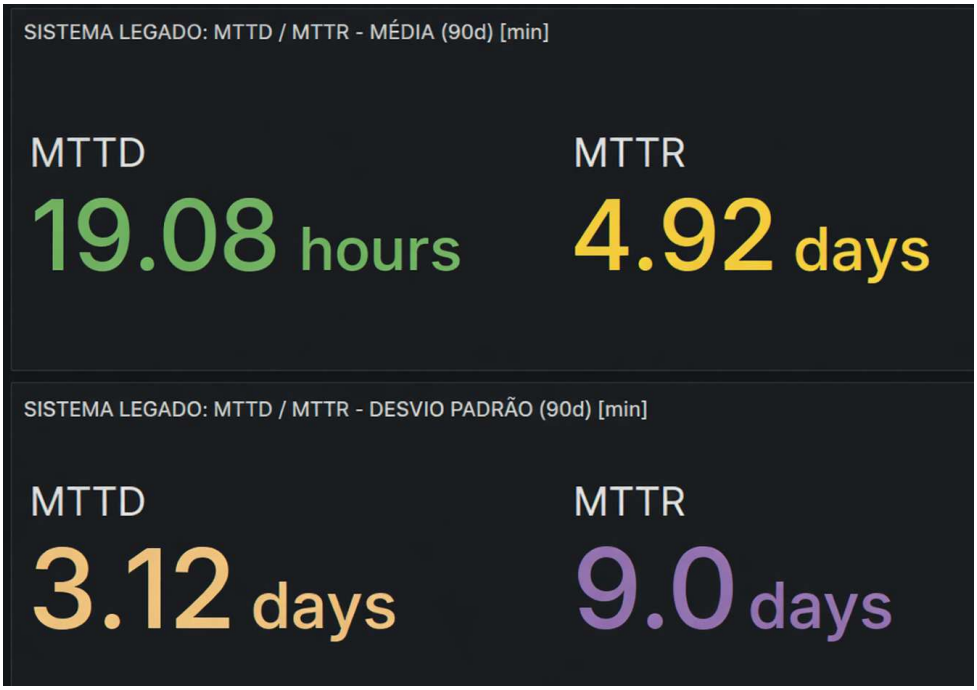


Figura 20 - Métricas média e mediana dos últimos 90 dias. Fonte: Autor.

Embora os resultados preliminares evidenciem ganhos operacionais relevantes, especialmente no que se refere à automação do fluxo de detecção e abertura de *tickets*, não foi possível mensurar os indicadores de MTTD e MTTR no período pós-implantação.

O tempo de operação do modelo automatizado ainda é insuficiente para compor uma amostra estatisticamente válida, o que inviabiliza comparações robustas com os valores obtidos no sistema legado.

Assim, os resultados apresentados referem-se exclusivamente ao cenário pré-implantação, constituindo uma linha de base inicial para avaliações futuras, quando uma janela temporal mais ampla permitir análises comparativas consistentes.

Apesar dos avanços observados na automatização do fluxo MGE, a solução apresenta limitações inerentes ao estágio atual de desenvolvimento. O modelo depende diretamente da qualidade e da completude dos dados gerados pelo ambiente monitorado, bem como da parametrização adequada das fontes de eventos e das funções de pertinência do motor Fuzzy.

Além disso, por se tratar de uma implantação piloto, a diversidade de cenários operacionais ainda não foi plenamente exercitada, o que reduz a observação de situações excepcionais e de condições-limite do processo automatizado.

Tais limitações são características naturais de projetos em fase inicial, conforme descrito nos ciclos iterativos de avaliação e refinamento propostos por [6], e tendem a ser mitigadas conforme o modelo amadurece, é aplicado a um conjunto mais amplo de ativos e opera sob diferentes condições institucionais.

Nesse sentido, os resultados devem ser interpretados à luz do escopo piloto, preservando-se sua utilidade como etapa fundamental na validação incremental do artefato.

6. DISCUSSÃO DOS RESULTADOS

Os resultados do piloto evidenciam um padrão central: a integração entre detecção automatizada (Zabbix), classificação adaptativa de criticidade (MIF com inferência Fuzzy) e gestão de *tickets* (GLPI) viabiliza a automação ponta a ponta do fluxo de Monitoração e Gerenciamento de Eventos (MGE), reduzindo etapas manuais na triagem e fortalecendo a padronização do tratamento dos eventos em consonância com o ITIL 4. A expressão mais clara desse padrão é a criação praticamente imediata do ticket após a detecção de um evento crítico, em contraste com o cenário anterior, no qual a abertura e a priorização dependiam de intervenção humana, com maior suscetibilidade a atrasos e variações de julgamento.

No piloto, em ambiente controlado, observou-se que o intervalo médio entre a detecção de um evento crítico e a criação do ticket no GLPI foi inferior a 1 minuto. Esse resultado reforça a capacidade do fluxo automatizado de reduzir atrasos associados à triagem manual e de tornar a resposta inicial menos dependente de variações de julgamento, ainda que a mensuração quantitativa sistemática de impacto em indicadores (p.ex., MTTD e MTTR) permaneça prevista para ciclos subsequentes.

Outro padrão recorrente refere-se ao contexto pré-implantação, caracterizado por um perfil predominantemente reativo de atendimento, refletido na linha de base estimada a partir de dados históricos (MTTD médio de 19,08 horas e MTTR médio de 4,92 dias, com 160 registros válidos em 90 dias, após o descarte de 49 chamados devido a inconsistências e incompletude dos dados registrados, que inviabilizavam o cálculo confiável das métricas). Esse diagnóstico fornece o enquadramento interpretativo para a relevância do acionamento automatizado do tratamento “logo após a geração do evento”, pois incide diretamente sobre o ponto inicial do encadeamento operacional, anteriormente dependente de análise manual para registrar e direcionar a demanda.

Ainda que o piloto aponte benefícios operacionais como redução de atrasos na abertura de *tickets* e maior consistência no encaminhamento inicial, os resultados desta etapa são exploratórios e baseiam-se em avaliação qualitativa e comparativa, assim, a quantificação do impacto em MTTD e MTTR permanece direcionada a ciclos posteriores. Nesse contexto, a interpretação deve distinguir entre: (*i*) evidências diretas do funcionamento integrado do fluxo (detectar → classificar → abrir/atualizar/encerrar ticket) e (*ii*) a inexistência, nesta etapa, de dados quantitativos suficientes para quantificar o ganho e afirmar, com rigor, que eventuais melhorias em MTTD/MTTR decorrem diretamente do modelo proposto.

Um segundo contraste concentra-se no núcleo decisório do modelo. A inferência Fuzzy substitui severidades fixas por uma classificação contínua baseada em impacto e urgência, ampliando a granularidade da priorização e reduzindo mudanças abruptas em situações limítrofes. Contudo, essa adaptatividade introduz uma exigência de governança: a qualidade da priorização depende da parametrização de impacto e urgência e do enriquecimento contextual por configuração externa, deslocando parte do esforço do código para a gestão e a manutenção do conhecimento operacional. Em termos práticos, o modelo tende a reduzir subjetividade na triagem pontual, mas requer disciplina de revisão e validação periódica dos parâmetros para sustentar consistência ao longo do tempo, aspecto coerente [108], ao destacarem que, no contexto municipal, a adoção de práticas ITIL 4 deve considerar a maturidade organizacional e a adaptação do modelo à realidade institucional.

Como evidência de operacionalização do modelo, no teste com o *host* "BORDA-02" o mapa de decisão configurado atribuiu impacto = 5 e urgência = 5, resultando em criticidade "Média" segundo os parâmetros definidos no piloto. Ressalta-se que tais valores são parametrizáveis e podem ser ajustados conforme políticas internas e contexto institucional, preservando a flexibilidade da abordagem em diferentes cenários.

Os achados são mais bem compreendidos como resultado de uma dinâmica de encadeamento operacional com mecanismos explícitos de controle. O Zabbix detecta e encaminha eventos ao MIF que normaliza os dados, aplica a inferência Fuzzy e integra-se ao GLPI para abrir ou atualizar *tickets* por meio de API e o GLPI consolida o registro do ciclo do incidente. O mecanismo de idempotência, sustentado pelo *event_id* como chave de controle, conecta confiabilidade técnica e governança ao reduzir duplicidades, eventos recorrentes atualizam o *ticket* existente, enquanto a recuperação do evento aciona o encerramento automatizado com registro de fechamento.

Adicionalmente, quando o Zabbix sinalizou a recuperação do evento, o próprio serviço realizou o encerramento automático do *ticket* (ID 291502), registrando o fechamento no GLPI. Esse comportamento reforça a consistência do ciclo operacional (abertura/atualização/encerramento) e a capacidade do modelo de lidar com variações de estado, contribuindo para rastreabilidade e redução de retrabalho.

Essa relação é decisiva para compreender o mecanismo operacional evidenciado no piloto, não se trata apenas de acelerar a abertura de *tickets*, mas de orquestrar o ciclo completo com consistência de estado (abrir/atualizar/encerrar) e trilha de auditoria. Adicionalmente, a geração automática de evidências no MIF e no GLPI amplia rastreabilidade e auditabilidade do processo, em alinhamento com requisitos de controle e evidência objetiva.

Por fim, a arquitetura modular desacoplada por APIs REST permite ajustes de parâmetros decisórios sem alteração do código-fonte, favorecendo adaptabilidade a diferentes contextos organizacionais. Em síntese, a articulação entre automação do fluxo, priorização contínua e controle de duplicidade/rastreabilidade descreve uma transição de um estado reativo e mais dependente de intervenção humana (*baseline*) para um fluxo operacional com maior padronização e evidência registrável, ainda que a quantificação dos efeitos permaneça planejada para etapas posteriores.

7. LIMITAÇÕES E TRABALHOS FUTUROS

A implantação em ambiente piloto permitiu demonstrar o funcionamento integrado do modelo, porém impõe limites naturais de generalização, uma vez que a avaliação ocorreu em um órgão municipal específico e com conjunto reduzido de ativos monitorados. Diante desse cenário, esta seção registra as principais restrições operacionais identificadas e organiza frentes de trabalhos futuros destinadas a apoiar a evolução do modelo, com foco em parametrização, calibração e monitoramento de indicadores.

Embora os resultados iniciais sejam promissores, a adoção do MGE em um município de grande porte ainda enfrenta restrições operacionais que requerem tratamento de riscos estruturado. A avaliação realizada neste estudo limitou-se a um órgão de saúde municipal, com um número reduzido de ativos monitorados. Como exemplo, estudos e análises recentes reforçam a complexidade e os desafios inerentes à implementação de CMDB, indicando que sua construção inicial não constitui um processo imediato.

De acordo com [109], pesquisas apontam que mais da metade dos esforços de CMDB se tornam incontroláveis, em especial quando há desalinhamento com o negócio, definição inadequada de escopo ou rigor insuficiente dos processos. Embora a Inteligência Artificial (IA) esteja sendo progressivamente integrada às soluções ITSM, os autores ressaltam que ainda é necessário trabalho adicional para que seu potencial seja plenamente alcançado no contexto do CMDB.

De modo semelhante, [110] enfatizam a crescente complexidade do gerenciamento da informação de infraestrutura em ambientes múltiplas nuvens (*multi-cloud*) e computação de borda (*edge computing),* destacando que a garantia de consistência e padronização de dados, alinhada a barreiras organizacionais como resistência à mudança, representam desafios críticos à integração eficaz do CMDB.

Revisões sistemáticas, como a de [83], confirmam que o processo de Gerenciamento de Configuração (CM) é frequentemente mal implementado e diretamente influenciado pela maturidade organizacional. Em organizações imaturas, prevalecem abordagens improvisadas e não padronizadas (*ad-hoc*), o que retarda a obtenção de benefícios. Os autores observam que, embora modelos de maturidade possam orientar melhorias, a evolução é lenta e pode demandar anos até atingir níveis superiores de maturidade.

Assim, ainda que os estudos não apresentem métricas temporais objetivas, como semanas ou meses, eles convergem em indicar que a implantação de CMDB constitui um processo prolongado, incremental e fortemente dependente da maturidade organizacional.

Como continuidade natural do estudo, pretende-se ampliar progressivamente o escopo de implantação do modelo, aumentando de forma incremental a quantidade de ativos e serviços monitorados até alcançar a cobertura do ambiente de TI do município. A estratégia recomendada é uma expansão por etapas, iniciando por secretarias e serviços prioritários e, em seguida, incorporando gradualmente novos conjuntos de ativos, incluindo a infraestrutura central do Datacenter, de modo a consolidar o uso do MGE em operação contínua e permitir avaliações em condições mais próximas do cenário real de produção. Para viabilizar essa ampliação com controle operacional e governança, os trabalhos futuros são organizados em três frentes integradas.

A primeira consiste em um assistente de parametrização gradual para apoiar as equipes na definição inicial de impacto e urgência por grupos de ativos, permitindo que o cadastro seja ampliado de forma progressiva por unidades e serviços. O caminho recomendado envolve um fluxo guiado dentro da central de serviços, conectado ao inventário e aos registros de ativos, com verificações e rastreamento das alterações realizadas. Como alternativa de menor esforço, podem ser utilizadas planilhas sob responsabilidade de cada unidade, com importação periódica para a central de serviços e validação por amostragem, reduzindo o esforço inicial sem alterar substancialmente as rotinas de trabalho.

A segunda frente refere-se à autocalibração das funções de pertinência com aprendizado supervisionado, ajustando, ao longo do tempo a combinação impacto x urgência a partir dos históricos da central de serviços, com objetivo de aperfeiçoar a priorização. O caminho recomendado prevê uma rotina que consome dados do *service desk*, gera novos parâmetros, realiza o versionamento de modelos e permite reversão quando necessário, operacionalizada em um fluxo automatizado de aprendizado de máquina (*pipeline de Machine Learning*). Como alternativa de menor complexidade, sugere-se uma revisão trimestral baseada em relatório de desvios entre a prioridade sugerida e a prioridade aplicada, seguida de ajuste manual das funções de pertinência, preservando a governança sem exigir *pipeline* automatizado.

A terceira frente compreende o desenvolvimento de painéis executivos em tempo real para consolidar criticidade média, volume de eventos e cumprimento de SLA, apoiando decisões de priorização de investimentos e alocação de recursos. O caminho

recomendado envolve a construção de *dashboards* conectados às fontes de monitoramento e ao *service desk*, com indicadores de tendência e detalhamento por unidade ou serviço.

Em síntese, os trabalhos futuros delineados nesta pesquisa convergem para o fortalecimento progressivo da escalabilidade, da precisão decisória e da capacidade gerencial do modelo proposto. A ampliação gradual da cobertura de ativos, o aperfeiçoamento da parametrização e da calibração das funções de pertinência, bem como o desenvolvimento de painéis executivos em tempo real, constituem etapas complementares de amadurecimento do GAIA-MGE. Sua implementação deverá considerar o nível de maturidade institucional, a disponibilidade de recursos técnicos e a necessidade de governança contínua, de modo a assegurar evolução controlada, rastreável e aderente às demandas do contexto organizacional.

8. CONCLUSÃO

Este estudo apresentou um modelo de automação para a prática de Monitoração e Gerenciamento de Eventos (MGE) que integra o Zabbix (detecção), um motor de inferência Fuzzy (MIF) para priorização e o GLPI (registro e rastreabilidade). O trabalho detalhou a arquitetura, o fluxo de dados e as rotinas de integração e demonstrou, por meio de um protótipo funcional, a automação do ciclo de tratamento associado aos eventos, desde o disparo do *trigger* até o encerramento do ticket, em conformidade com as diretrizes do ITIL 4.

A utilização da lógica Fuzzy, fundamentada nos trabalhos de [2], [3] e [4], mostrou-se adequada em ambiente piloto ao produzir valores contínuos de criticidade posteriormente mapeados para níveis linguísticos. Essa abordagem apresenta maior granularidade do que mecanismos baseados em limiares binários, como a lógica OK/Problem de *trigger*s booleanos descrita na documentação do Zabbix [101], favorecendo priorizações mais alinhadas ao contexto operacional e, consequentemente, decisões de resposta mais assertivas.

Do ponto de vista de aplicabilidade, embora a proposta tenha sido direcionada ao setor público, o modelo é replicável também em organizações privadas, pois sua construção modular, baseada em APIs REST e componentes de código aberto, facilita a adaptação a diferentes cenários. Limitações operacionais, como o esforço inicial de parametrização de ativos e a necessidade de manutenção contínua da base de configuração, podem ser mitigadas em trabalhos futuros por meio de autocalibração das funções de pertinência e de assistentes de parametrização incremental.

De maneira complementar, como a implantação ocorreu em ambiente piloto, a avaliação contemplou apenas um recorte operacional, o que reforça a necessidade de expandir validações futuras para cenários mais amplos e heterogêneos. Nesse contexto, estudos envolvendo outros municípios, com diferentes níveis de maturidade em governança de TIC, podem aprofundar a análise do desempenho do modelo e testar sua adaptabilidade a realidades administrativas diversas.

Por fim, destaca-se que a arquitetura desenvolvida possui caráter modular, parametrizável e inteiramente baseado em ferramentas abertas, o que reforça sua replicabilidade e potencial de adoção em diferentes contextos institucionais.

9. CONTRIBUIÇÕES DA PESQUISA

A principal contribuição deste trabalho para a Ciência da Computação reside na proposição de um modelo integrado de Monitoração e Gerenciamento de Eventos que combina, de forma coerente e operacional, elementos investigados de maneira fragmentada na literatura: modelagem de processos em BPMN, monitoração contínua baseada em NMS, inferência Fuzzy multicritério, mecanismos de idempotência e automação do ciclo de vida de *tickets* em ferramenta ITSM. Essa convergência técnica e conceitual resulta em um artefato que supera abordagens tradicionais ao estabelecer um fluxo end-to-end capaz de detectar, classificar, priorizar e tratar eventos de TI de maneira padronizada, adaptativa e alinhada ao ITIL 4, com impacto na qualidade e na eficiência dos serviços.

Do ponto de vista metodológico, o modelo contribui ao demonstrar como práticas consolidadas de engenharia de software, governança de TI e inteligência computacional podem ser articuladas em uma solução aplicada, validada em ambiente real e sustentada por princípios formais de modelagem e decisão. A utilização combinada de BPMN, inferência Fuzzy e automação acoplada ao Zabbix e ao GLPI oferece uma estrutura replicável e extensível, reforçando a relevância de estudos que aproximam teoria e prática em contextos operacionais complexos, como administrações públicas de grande porte. Ao incorporar idempotência ao pipeline de eventos, aspecto ausente nos trabalhos correlatos, o modelo também avança na confiabilidade e consistência dos processos automatizados.

No âmbito do mestrado, o trabalho se destaca por apresentar uma contribuição aplicável, replicável, adaptativa e metodologicamente robusta, alinhada às expectativas da pesquisa profissional e às demandas reais de gestão inteligente de operações de TI. O artefato desenvolvido não apenas demonstra viabilidade técnica, mas também oferece uma base científica para estudos futuros, possibilitando extensões em direção a sistemas autonômicos, análise preditiva, governança adaptativa e integração com arquiteturas orientadas a eventos. Dessa forma, o modelo proposto eleva o nível de maturidade institucional e amplia o escopo da pesquisa aplicada em engenharia de sistemas e gestão de serviços de TI.

Para a instituição, o modelo proposto representa um avanço substancial na profissionalização da gestão de operações de TI, ao estabelecer um fluxo automatizado, padronizado e mensurável de monitoramento e tratamento de eventos. A integração entre BPMN, Zabbix, motor Fuzzy multicritério, idempotência e GLPI reduz tempos de detecção e resposta, elimina redundâncias operacionais, qualifica a priorização de incidentes e fortalece a

rastreabilidade e a transparência dos processos. Em um cenário municipal caracterizado por equipes reduzidas e alta demanda por disponibilidade de serviços públicos digitais, o modelo contribui diretamente para o aumento da maturidade institucional, para a mitigação de riscos operacionais e para a melhoria contínua dos serviços de TI prestados à sociedade.

Adicionalmente, a pesquisa entrega um conjunto de artefatos *open source*, alinhados às boas práticas do ITIL 4 [1] e às recomendações normativas [51], documentados e disponíveis à comunidade, bem como evidências empíricas iniciais de que a integração entre ZABBIX, MIF e GLPI possui potencial para reduzir MTTD e MTTR. Esses elementos reforçam a relevância prática do modelo e sua capacidade de ser replicado e adaptado em outros contextos institucionais, incluindo municípios de diferentes portes e organizações privadas.

10. DISPONIBILIDADE DE DADOS E ARTEFATOS

Os conjuntos de dados, planilha de métricas do sistema legado com MTTD e MTTR, scripts de análise, diagramas e demais artefatos que sustentam a descrição do modelo proposto de integração entre Zabbix, MFI e GLPI estão disponíveis em repositório digital de acesso aberto[6], com o objetivo de promover transparência, reprodutibilidade e possibilitar extensões futuras da pesquisa.

[6] Disponível em: *https://figshare.com/s/bfd647f9379b14c36dfc*

11. CONSIDERAÇÕES DE ÉTICA

Este estudo utilizou exclusivamente dados técnicos de infraestrutura de TIC, referentes a ativos reais em produção, coletados por instâncias piloto (ZABBIX e GLPI) em ambiente isolado. Os registros foram anonimizados, não contêm dados pessoais e estão em conformidade com a LGPD (Lei 13.709/2018)[7] e as normas locais de segurança. Como não houve participação de seres humanos nem uso de informações sensíveis, não se exigiu submissão a Comitê de Ética em Pesquisa.

[7] Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

REFERÊNCIAS

[1] Axelos, *ITIL ® Foundation ITIL 4 Edition*, 1st ed. The Stationery Office (TSO), 2019.

[2] L. A. Zadeh, "Fuzzy sets," *Information and Control*, vol. 8, no. 3, pp. 338–353, 1965.

[3] H.-J. Zimmermann, *Fuzzy Set Theory — and Its Applications*, 4th ed. Boston, MA: Springer, 2001.

[4] E. Cox, *The Fuzzy Systems Handbook*. Boston, MA, USA: AP Professional, 1994.

[5] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004, doi: 10.2307/25148625.

[6] K. Peffers, T. Tuunanen, M. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management Information Systems*, vol. 24, pp. 45–77, 2007.

[7] M. I. Sarwar, Q. A. Niazi, T. Alyas, and T. Alghamdi, "Digital Transformation of Public Sector Governance With IT Service Management—A Pilot Study," *IEEE Access*, vol. 11, pp. 6490–6512, 2023, doi: 10.1109/ACCESS.2023.3237550.

[8] H. Gunawan, A. B. P. Irianto, and J. G. P. Negara, "Implementation of Sustainable Service Improvement in Organizations Using ITIL Framework," in *Procedia Computer Science*, 2024, pp. 748–755. doi: 10.1016/j.procs.2024.03.061.

[9] M. Mora and others, "The role of decision-making support systems in IT service management processes," *Intelligent Decision Technologies*, vol. 8, no. 2, pp. 147–163, 2014.

[10] D. Das, "A proactive event-management framework for cloud services," in *Proc.\ 12th IEEE Int.\ Conf.\ on Cloud Computing*, 2019, pp. 123–130. doi: 10.1109/CLOUD.2019.XXXXXX.

[11] S. de Governo Digital, "Mapa de Governo Digital – Boletim 2022," Brasília, Brasil, 2022.

[12] M. A. E. Araújo, "Gênios: Framework para Planejamento Visual de TI Utilizando Arquitetura Corporativa," Universidade Federal de Pernambuco, 2020. [Online]. Available: http://cin.ufpe.br/~posgraduacao

[13] E. Przeybilovicz, M. A. Cunha, and F. de S. Meirelles, "O uso da tecnologia da informação e comunicação para caracterizar os municípios: quem são e o que precisam para desenvolver ações de governo eletrônico e smart city," *Revista de Administração Pública*, vol. 52, no. 4, pp. 630–649, 2018, doi: 10.1590/0034-7612170582.

[14] J. B. Silva, M. A. Costa, and A. P. Oliveira, “ITIL 4 adoption in Brazilian public organizations: impacts on efficiency and service quality,” *J. Inf. Syst. Public Admin.*, vol. 12, no. 1, pp. 25–40, 2020.

[15] Q. Yu *et al.*, “A survey on intelligent management of alerts and incidents in IT services,” *Journal of Network and Computer Applications*, vol. 224, p. 103842, 2024, doi: 10.1016/j.jnca.2024.103842.

[16] J. Luftman, “Assessing IT/business alignment,” *Information systems management*, vol. 20, no. 4, pp. 9–15, 2003.

[17] Y. Al-Ashmoery *et al.*, “Impact of Integrating Lean, Agile, and DevOps with ITIL4 Framework for Modern IT Service Management,” in *2024 1st International Conference on Emerging Technologies for Dependable Internet of Things (ICETI)*, 2024, pp. 1–8.

[18] ISACA, *COBIT 2019 Framework: Governance and Management Objectives*. USA: Information Systems Audit and Control Association, 2018.

[19] H. İ. Karataş and Ö. Çakır, “A Systematic Literature Review on IT Governance Mechanisms and Frameworks,” *Journal of Learning and Teaching in Digital Age*, vol. 9, no. 1, pp. 88–101, 2024, doi: 10.53850/joltida.1300262.

[20] K. Santos and Á. Moura, “Características essenciais da governança de TI: uma revisão sistemática de literatura,” *Revista Gestão e Conhecimento Contemporâneo*, vol. 3, no. 1, pp. 45–68, 2024.

[21] B. Jaeger, “It governance in local governments,” in *ECDG 2018 18th European Conference on Digital Government*, 2018, p. 95.

[22] G. M. Jonathan and L. Rusu, “IT governance in public organizations: a systematic literature review,” *International Journal of IT/Business Alignment and Governance (IJITBAG)*, vol. 9, no. 2, pp. 30–52, 2018.

[23] I. L. M. de Sena, “Governança de TI em órgãos públicos: um mapeamento sistemático da literatura,” Universidade Federal de Pernambuco - UFPE, 2018. [Online]. Available: https://repositorio.ufpe.br/handle/123456789/34219

[24] C. Sengik and G. Lunardi, “Benefits of ITIL-based service management in the Brazilian public sector,” *iSys – Revista Brasileira de Sistemas de Informação*, vol. 16, no. 2, pp. 45–60, 2023.

[25] A. Peralta, J. A. Olivas, P. Navarro-Illana, and J. Alvarado, “A Hybrid Mathematical Framework for Dynamic Incident Prioritization Using Fuzzy Q-Learning and Text Analytics,” *Mathematics*, vol. 13, no. 12, p. 1941, 2025, doi: 10.3390/math13121941.

[26] S. Sharmin and R. H. Chowdhury, “Digital transformation in governance: The impact of e-governance on public administration and transparency,” *Journal of Computer Science and Technology Studies*, vol. 7, no. 1, pp. 362–379, 2025.

[27] L. A. Costa, A. Fontão, and R. Santos, “PSECO-IM: An Approach for Incident Management to Support Governance in Proprietary Software Ecosystems,” in *Anais Estendidos do XVIII Simpósio Brasileiro de Sistemas de Informação (SBSI 2022)*, 2022, pp. 130–132. doi: 10.5753/sbsi_estendido.2022.222264.

[28] L. Topin, E. Borges, and L. Ribeiro, “Uma abordagem para adequação de serviços baseada em práticas da ITIL,” in *Anais do XIII Simpósio Brasileiro de Sistemas de Informação (SBSI 2017)*, 2017, pp. 579–584. doi: 10.5753/sbsi.2017.6090.

[29] D. Dzemydienė, S. Turskienė, and I. Šileikienė, “Development of ICT infrastructure management services for optimization of administration of educational institution activities by using ITIL-v4,” *Baltic journal of modern computing.*, vol. 11, no. 4, pp. 558–579, 2023.

[30] L. Magnusson, S. Iqbal, P. Elm, and F. Dalipi, “Information Security Governance in the Public Sector: Investigations, Approaches, Measures, and Trends,” *Int. J. Inf. Secur.*, vol. 24, no. 2, pp. 177–200, 2025, doi: 10.1007/s10207-025-01097-x.

[31] “Date: December 2013 Business Process Model and Notation (BPMN) Version 2.0.2 NOTE: Version 2.0.2 contains a minor change to Clause 15. OMG Document Number: formal/2013-12-09 Standard document URL: http://www.omg.org/spec/BPMN Machine consumable files,” 2010.

[32] M. T. Garcia, “Medição de similaridade estrutural entre modelos de processo de negócio em BPMN 2.0: uma extensão incluindo loops e elementos complexos da notação,” Universidade de São Paulo, São Paulo, 2022. doi: 10.11606/D.100.2022.tde-21112022-094808.

[33] I. Aguilar-Alonso, M. P. Pascal, and C. M. Macias, “Applying business process modeling to improve IT incident management processes in a public entity in Peru,” *Journal of Software and Systems Development*, vol. 2020, pp. 1–20, 2020.

[34] T. Tavantzis, R. Promikyridis, and E. Tambouris, “Towards exploiting BPMN and DMN in public service modeling,” in *Proceedings of the 27th Pan-Hellenic Conference on Progress in Computing and Informatics*, 2023, pp. 211–216.

[35] M. Dumas, L. M. Rosa, J. Mendling, and A. H. Reijers, *Fundamentals of business process management*. Springer, 2018.

[36] J. Becker, R. Knackstedt, and J. Pöppelbuß, “Developing maturity models for IT management: A procedure model and its application,” *Business & information systems engineering*, vol. 1, no. 3, pp. 213–222, 2009.

[37] P. O. L. dos Santos, A. P. B. da Silva, J. Souza, and R. T. de Sousa, “Proposta de construção de modelo de maturidade em governança e gestão de TIC,” *REAd. Revista Eletrônica de Administração (Porto Alegre)*, vol. 26, no. 02, pp. 463–494, 2020.

[38] J. Souza Neto and L. E. M. de Carvalho, “A avaliação da governança de TI da administração pública sob a ótica dos princ\’\ipios da governança corporativa,” 2020.

[39] E. H. Mamdani and S. Assilian, “An experiment in linguistic synthesis with a fuzzy logic controller,” *Int. J. Man. Mach. Stud.*, vol. 7, no. 1, pp. 1–13, 1975.

[40] N. Tomak and F. Polat, “A fuzzy multi-criteria model for risk prioritization in incident management,” *Comput. Ind. Eng.*, vol. 168, p. 108030, 2022, doi: 10.1016/j.cie.2022.108030.

[41] L. V Olano and others, “Prioritization of incident management process using ITIL-fuzzy for informatics development sector of private universities,” *Int. J. Fuzzy Logic Intell. Syst.*, vol. 25, no. 1, pp. 37–54, 2025, doi: 10.5391/IJFIS.2025.25.1.37.

[42] G. Pascarella and others, “Risk analysis in healthcare organizations: Methodological framework and critical variables,” *Risk Manag. Healthc. Policy*, vol. 14, pp. 2897–2911, 2021, doi: 10.2147/RMHP.S309098.

[43] R. L. Keeney and H. Raiffa, *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*. Cambridge: Cambridge University Press, 1993.

[44] G. Project, “GLPI Documentation,” 2025.

[45] D. MacLean and J. Frowley, “Implementation and impacts of IT Service Management in organisations,” *Information & Management*, vol. 60, no. 4, p. 104238, 2023, doi: 10.1016/j.im.2023.104238.

[46] N. Crosley and I. Wasito, “Improving IT Support Efficiency Using AI-Driven Ticket Random Forest Classification Technique,” *Sinkron*, vol. 8, no. 4, pp. 2283–2293, 2023, doi: 10.33395/sinkron.v8i4.12925.

[47] B. Waseso, M. A. Nugroho, and R. P. Sari, “Agile methodologies in IT service management,” in *Proceedings of the 2024 International Conference on Information Technology Systems and Innovation (CITSM 2024)*, IEEE, 2024, pp. 1–6. doi: 10.1109/CITSM64103.2024.10775478.

[48] R. T. Fielding, “Architectural Styles and the Design of Network-based Software Architectures,” University of California, Irvine, 2000. [Online]. Available: https://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm

[49] M. Fowler, *Patterns of Enterprise Application Architecture*. Boston, MA: Addison-Wesley Professional, 2002.

[50] S. Newman, *Building Microservices*. Sebastopol, CA: O’Reilly Media, 2015.

[51] “ISO/IEC 20000-1:2018 — Service Management System Requirements,” 2018.

[52] K. K. Pappula, S. Anasuri, and G. P. Rusum, “Building Observability into Full-Stack Systems: Metrics That Matter,” *International Journal of Emerging Research in Engineering and Technology*, vol. 2, no. 4, pp. 48–58, 2021.

[53] O. B. Johnson, J. Olamijuwon, E. Cadet, O. S. Osundare, and Y. W. Weldegeorgise, “Developing real-time monitoring models to enhance operational support and improve incident response times,” *Int J Eng Res Dev*, vol. 20, no. 11, pp. 1296–1304, 2024.

[54] S. Żurawski, A. Chrzaszcz, Z. Ciekanowski, Y. Pauliuchuk, S. Pietrzyk, and B. Wyrzykowska, “Effectiveness of information security incident management systems: identifying practices, challenges and development perspectives,” 2025.

[55] A. I. Aguilar and R. Li, “Responsibility Assignment Matrix in Responding to Critical Outages: A Case Study of IT Incident Management Activity Process Design,” in *Proceedings of the ACM Conference on Computer and Information Science*, New York, NY, USA: Association for Computing Machinery (ACM), 2023. doi: 10.1145/3603955.3603956.

[56] G. Nguyen, S. Dlugolinsky, V. Tran, and Á. López García, “Network security AIOps for online stream data monitoring,” *Neural Comput. Appl.*, vol. 36, no. 14925–14949, 2024, doi: 10.1007/s00521-024-09863-z.

[57] L. Tao *et al.*, “Real-Time Anomaly Detection for Large-Scale Network Devices,” *IEEE Transactions on Networking*, 2025, doi: 10.1109/TON.2025.3529861.

[58] Y. Klots, V. Titova, N. Petliak, D. Tymoshchuk, and N. Zagorodna, “Intelligent data monitoring anomaly detection system based on statistical and machine learning approaches,” 2025.

[59] A. Peralta, J. A. Olivas, and P. Navarro-Illana, “A Fuzzy Logic Framework for Text-Based Incident Prioritization: Mathematical Modeling and Case Study Evaluation,” *Mathematics*, vol. 13, no. 12, p. 2014, 2025.

[60] M. Mrówczyńska *et al.*, “A new fuzzy model of multi-criteria decision support based on Bayesian networks for the urban areas’ decarbonization planning,” *Energy Convers. Manag.*, vol. 268, p. 116035, 2022.

[61] R. Pereira, I. Bianchi, A. L. Martins, J. B. de Vasconcelos, and Á. Rocha, “Business process modelling to improve incident management process,” in *World Conference on Information Systems and Technologies*, 2020, pp. 689–702.

[62] A. R. Teixeira, J. V. Ferreira, and A. L. Ramos, “Optimization of Business Processes Through BPM Methodology: A Case Study on Data Analysis and Performance Improvement,” *Information*, vol. 15, no. 11, p. 724, 2024, doi: 10.3390/info15110724.

[63] J. T. Licardo, N. Tanković, and D. Etinger, “A method for extracting bpmn models from textual descriptions using natural language processing,” *Procedia Comput. Sci.*, vol. 239, pp. 483–490, 2024.

[64] M. Khmelyarchuk, S. Zhukovska, G. Weigang, and K. Myronchuk, “BPMN Diagrams as an Essential Tool for Enhancing Business Process Management and Team Collaboration,” *European Research Studies Journal*, vol. XXVII, no. S2, pp. 652–682, 2024.

[65] T. Reis, P. Leite, and R. Barros, “Implantação do Zabbix na UFAL Campus Arapiraca,” in *Anais ERI-GO*, 2020.

[66] A. Mosteiro V’azquez, C. Dafonte, and ’Angel G’omez, “Open source monitoring system for it infrastructures incorporating iot-based sensors,” in *Proceedings*, 2020, p. 56.

[67] C. F. Matte, G. Langwinski, L. S. Cardoso, and A. Bussador, “Comparação de Ferramentas para Monitoramento de Redes de Computadores em Ambientes Simulados,” in *Congresso Latino-Americano de Software Livre e Tecnologias Abertas (Latinoware)*, 2022, pp. 129–132.

[68] F. Guo, C. Chen, and K. Li, “Research on Zabbix Monitoring System for Large-scale Smart Campus Network from a Distributed Perspective,” *J. Electr. Syst*, vol. 20, no. 10, pp. 631–648, 2024.

[69] G. B. Rodrigues, I. A. D. Bernardina, P. Í. da S. Hermes, G. V. Carneiro, and E. de S. Magalhães, “Zabbix na TI hospitalar: eficiência operacional e cuidado ao paciente,” *Revista Esfera Acadêmica Tecnologia*, vol. 9, no. 1, pp. 1–20, 2024.

[70] Leite, “Aplicação de Inferência Fuzzy para Tomada de Decisão em Processos de SMT no Polo Industrial de Manaus,” *IOSR Journal of Business and Management (IOSR-JBM)*, vol. 26, no. 12, Ser. 9, pp. 58–65, 2024, doi: 10.9790/487X-2612095865.

[71] R. F. F. de Oliveira, V. E. R. Costa, R. B. Ribeiro, B. D. da Silva, J. M. S. das Neves, and S. T. dos Santos Neto, “LÓGICA FUZZY E INTELIGÊNCIA ARTIFICIAL: A REVOLUÇÃO DA QUALIDADE NA MANUFATURA ENXUTA,” *Revista Contemporânea*, vol. 5, no. 7, pp. e8708–e8708, 2025.

[72] T. Fujita, “A Proposed Framework for Fuzzy and NeutrosophicExtensions of Service Integration and Management (SIAM) and ITIL-Based Models,” *Journal of Intelligent Decision Making and Granular Computing*, vol. 1, no. 1, pp. 161–198, 2025.

[73] I. Ranggadara, “Fuzzy Tsukamoto and ITIL for improvement strategy on incident ticket services,” *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 10, pp. 897–903, 2019.

[74] K. Slavyanov and R. Dimov, “Application of fuzzy logic in cybersecurity decision making and analysis after a cyber incident detection,” in *ENVIRONMENT. TECHNOLOGIES. RESOURCES. Proceedings of the International Scientific and Practical Conference*, 2024, pp. 259–263.

[75] W. Funika, F. Szura, and J. Kitowski, “Automation of system monitoring based on fuzzy logic or rules; comparison of two designed approaches with regard to computational infrastructures,” in *Building a National Distributed e-Infrastructure–PL-Grid: Scientific and Technical Achievements*, Springer, 2012, pp. 142–156.

[76] M. Alfarhan, M. Kamel, and M. Saleh, “IT Services Evaluation Model Based on Fuzzylogic,” *International Journal of Computer Trends and Technology (IJCTT)*, vol. 57, no. 1, pp. 35–43, 2018, [Online]. Available: http://www.ijcttjournal.org

[77] X. Gu, G. Howells, and H. Yuan, “A soft prototype-based autonomous fuzzy inference system for network intrusion detection,” *Inf. Sci. (N. Y).*, vol. 677, p. 120964, 2024.

[78] S. A. Abdullah and A. S. Al-Hashmi, “TiSEFE Time series evolving fuzzy engine for network traffic classification,” *International Journal of Communication Networks and Information Security*, vol. 10, no. 1, pp. 116–124, 2018.

[79] I. L. B. Vasconcellos, “Central de Serviços: uma análise das ferramentas OTRS, GLPI, RT e OcoMon,” in *Congresso de Tecnologia da Informação*, 2017.

[80] J. Liu *et al.*, “Incident-aware Duplicate Ticket Aggregation for Cloud Systems,” in *Proceedings - International Conference on Software Engineering*, IEEE Computer Society, Jul. 2023, pp. 2299–2311. doi: 10.1109/ICSE48619.2023.00193.

[81] Z. Chen *et al.*, “Graph-based incident aggregation for large-scale online service systems,” in *2021 36th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, 2021, pp. 430–442.

[82] N. Achmad and H. Muhaimin, “Ticket Prediction using LSTM on a GLPI System,” *International Journal of Open Information Technologies*, vol. 11, no. 7, pp. 118–121, 2023.

[83] M. Serrano and G. Pereira, “Adoção e maturidade do Gerenciamento de Configuração: uma revisão sistemática,” *Revista de Administração e Sistemas de Informação*, vol. 17, no. 3, pp. 234–251, 2020.

[84] R. Yandri, D. N. Utama, A. Zahra, and others, “Evaluation model for the implementation of information technology service management using fuzzy ITIL,” *Procedia Comput. Sci.*, vol. 157, pp. 290–297, 2019.

[85] W. H. Ueno and R. M. de Barros, “Case Study of the Gaia Maturity Model to Deploy IT Services Continuity,” in *Proceedings of the 15th CONTECSI International Conference on Information Systems and Technology Management*, 2018, pp. 1569–1581. doi: 10.5748/9788599693148-15contecsi/ps-5695.

[86] R. K. Yin, *Case study research and applications*, vol. 6. Sage Thousand Oaks, CA, 2018.

[87] UEL Universidade Estadual de Londrina, “Paraná Smart City - Governança em TI,” 2025. [Online]. Available: https://gaia2.uel.br/

[88] J. W. Creswell and V. L. P. Clark, *Designing and Conducting Mixed Methods Research*, 3rd ed. Thousand Oaks, CA: SAGE Publications, 2017.

[89] A. C. Gil, *Métodos e Técnicas de Pesquisa*, 8th ed. São Paulo: Atlas, 2019.

[90] J. B. Silva, M. A. Costa, and A. P. Oliveira, “Adopting ITIL 4 in Brazilian public organizations: impacts on efficiency and service quality,” *Journal of Information Systems in Public Administration*, vol. 12, no. 1, pp. 25–40, 2020.

[91] A. S. Markowski, M. S. Mannan, and A. Bigoszewska, “Fuzzy logic for process safety analysis,” *J. Loss Prev. Process Ind.*, vol. 22, no. 6, pp. 695–702, 2009.

[92] D. Nagy, A. M. Yassin, and A. Bhattacherjee, “Organizational adoption of open source software: barriers and remedies,” *Commun. ACM*, vol. 53, no. 3, pp. 148–151, 2010, doi: 10.1145/1666420.1666457.

[93] “2021_R. D. P. Suhanda and D. Pratami, RACI Matrix Design for Managing Stakeholders in Project Case Study of PT. XYZ.bib”.

[94] J. Iden and T. R. Eikebrokk, “Using the ITIL process reference model for realizing IT Governance: An empirical investigation,” *Information Systems Management*, vol. 31, no. 1, pp. 37–58, 2014, doi: 10.1080/10580530.2014.854033.

[95] W. P. S. Lemos and G. C. Ana, “Metodologia Científica: a pesquisa qualitativa nas visões de Lüdke e André,” *Revista Eletrônica Científica Ensino Interdisciplinar*, vol. 4, no. 12, 2018.

[96] R. Likert, “A Technique for the Measurement of Attitudes,” *Archives of Psychology*, vol. 22, no. 140, pp. 1–55, 1932, [Online]. Available: https://legacy.voteview.com/pdf/Likert_1932.pdf

[97] A. Joshi, S. Kale, S. Chandel, and D. Pal, “Likert Scale: Explored and Explained,” *Current Journal of Applied Science and Technology*, vol. 7, no. 4, pp. 396–403, 2015, doi: 10.9734/BJAST/2015/14975.

[98] C. A. B. Oliveira, “Governança de TI: Modelos de maturidade e sua aplicação,” *Revista de Administração e Inovação*, vol. 15, no. 3, pp. 122–145, 2018.

[99] G. U. Briganó, “Um framework para desenvolvimento de governança de TIC,” Universidade Estadual de Londrina – UEL, 2012.

[100] C. A. Brewer, *Color Use Guidelines for Mapping and Visualization*. Elsevier, 1994.

[101] Zabbix LLC, “Zabbix Documentation 7.0,” 2025.

[102] A. S. Markowski and M. S. Mannan, “Application of Fuzzy logic to explosion risk assessment,” *J. Hazard. Mater.*, vol. 108, no. 1–2, pp. 41–62, 2004, doi: 10.1016/j.jhazmat.2003.07.004.

[103] N. Tomak and T. K. Polat, “Risk prioritization model driven by success factor in the light of multicriteria decision making,” 2022.

[104] D. Z. Šaletić, D. M. Velašević, and N. E. Mastorakis, “The influence of shapes of Fuzzy sets membership functions on Fuzzy system performances,” in *Proc. 3rd World Multiconf. on Circuits, Systems, Communications and Computers (CSCC)*, Athens, Greece, 1999, pp. 1131–1135.

[105] T. J. Ross, *Fuzzy Logic with Engineering Applications*, 3rd ed. Hoboken: John Wiley & Sons, 2010.

[106] B. De Baets, “Generalized Idempotence in Fuzzy Mathematical Morphology,” in *Fuzzy Techniques in Image Processing*, vol. 52, E. E. Kerre and M. Nachtegael, Eds., in Studies in Fuzziness and Soft Computing, vol. 52. , Heidelberg: Physica–Springer, 2000, pp. 58–75. doi: 10.1007/978-3-7908-1847-5_2.

[107] M. M. Botezatu, J. Bogojeska, I. Giurgiu, H. Voelzer, and D. Wiesmann, “Multi-view incident ticket clustering for optimal ticket dispatching,” in *Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2015, pp. 1711–1720.

[108] R. Miranda De Barros, V. T. De Oliveira Barros, and V. Mantovani, “A Performance and Capacity Monitoring Model based on ITIL 4: A case study applied in a City Hall.”

[109] R. Dande, F. Silva, and L. Moreira, “Desafios e perspectivas na gestão de CMDB com integração de IA: uma revisão de literatura,” *Revista Brasileira de Gestão e Tecnologia*, vol. 25, no. 2, pp. 115–133, 2024.

[110] J. Tawo and K. Ajayi, “CMDB Integration in Multi-cloud and Edge Environments: Challenges and Opportunities,” in *Proceedings of the International Conference on Cloud Management*, 2025, pp. 45–54.

Apêndices

APÊNDICE A – ESPECIFICAÇÃO DO MODELO PROPOSTO

Este apêndice apresenta a descrição detalhada dos fluxos: 1.0 MGE automático completo, 2.0 MGE manual, 3.0 Plano de Monitoração, 4.0 Monitorar e 5.0 MGE automático (apenas exceção), modelados em BMPN. Para cada fluxo são apresentadas: (*i*) a descrição; (*ii*) os atores envolvidos; (*iii*) as etapas); (*iv*) os recursos; (*v*) as entradas; (*vi*) as ações; e (*vii*) as saídas. O material constitui referência técnica para a implantação do modelo, assegurando maior transparência, rastreabilidade e otimização dos processos operacionais.

1.1 Coletar Métricas Logs Status de Ativos
Descrição:
Coleta automatizada ou semiautomatizada de dados operacionais dos ativos monitorados. Inclui logs, métricas e status, com base no plano de monitoramento.
Atores Envolvidos:
- Sistema de Monitoramento. - Analista de TI (caso haja falhas ou ajustes).
Etapas:
Se implantado: a) Acesso automatizado aos ativos conforme plano; b) Coleta periódica ou contínua dos dados. Se não implantado (considera-se o mínimo necessário): a) Acesso manual aos ativos; b) Extração de logs ou métricas pontuais (ex: via SSH, painel do roteador, outros); c) Armazenamento manual em planilha (ex: excel).
Recursos:
Se implantado: a) Ferramenta integrada (ex: Zabbix) com inventário, base de conhecimento e plano de monitoramento. Se não implantado (considera-se o mínimo necessário): a) acesso técnico ao ativo e capacidade de extrair os dados.
Entrada:
- Base de Conhecimento. - Inventário de Ativos. - Plano de Monitoramento.
Ação:
Coletar os dados do ativo (automática ou manualmente).
Saída:
Dados prontos para correlação (1.2).
1.2 Correlacionar Eventos e Identificar Padrões
Descrição:

Aplicação de filtros de relevância e lógica de correlação entre eventos para eliminar redundâncias e identificar padrões anômalos.
Atores Envolvidos:
- Sistema de Monitoramento. - Analista de TI (em revisão).
Etapas:
Se implantado: a) Aplicação automática de regras de correlação; b) Geração de evento consolidado. Se não implantado (considera-se o mínimo necessário): a) Leitura manual dos dados coletados; b) Verificação de repetições ou falhas similares; c) Registro manual do evento em planilha.
Recursos:
Se implantado: a) Ferramenta com mecanismo de correlação automatizada, capaz de agrupar eventos por tempo, tipo, causa ou dependência (ex: *triggers*, regras de agrupamento, *templates* na ferramenta de monitoramento (ex: Zabbix). Se não implantado (considera-se o mínimo necessário): a) Logs e planilha para controle.
Entrada:
Dados operacionais coletados (1.1).
Ação:
Correlacionar eventos e filtrar informações irrelevantes.
Saída:
Evento classificado como: • 1.3 Informativo; • 1.4 Alerta; • 1.5 Exceção.
1.3 Informativo
Descrição:
Evento sem impacto no serviço. É registrado apenas para fins estatísticos, históricos ou de auditoria.
Atores Envolvidos:
- Sistema de Monitoramento. - Analista de TI ou responsável pela Auditoria (caso necessário).
Etapas:
Se o processo estiver implantado: a) Evento classificado automaticamente como informativo pela ferramenta; b) Marcado como “sem impacto” ou “resolvido”; c) Encaminhado automaticamente para registro histórico (1.6). Se o processo não estiver implantado (considera-se o mínimo necessário): a) Técnico avalia manualmente os dados e decide se há ou não impacto; b) Se não houver, registra o evento como “informativo” em planilha ou documento interno; c) Encaminha para arquivamento manual (1.6);

d) Se houver impacto, avalia se encaminha para 1.4 ou 1.5.
Recursos:
Se implantado: a) Base de dados de eventos históricos. Se não implantado: a) Registro mínimo em planilha ou ferramenta.
Entrada:
Evento classificado como informativo após correlação (1.2).
Ação:
Encaminhar para registro, sem ação corretiva
Saída:
Evento armazenado para rastreabilidade (1.6).
1.4 Alerta
Descrição:
Indica que um limite técnico foi atingido. (ex: uso de CPU elevado, resposta lenta) mas ainda não representa uma falha ativa. Requer atenção e análise para prevenir impactos.
Atores Envolvidos:
- Sistema de Monitoramento. - Analista de TI.
Etapas:
Se o processo estiver implantado: a) Evento é automaticamente classificado como “alerta” pela ferramenta, com base nas regras configuradas (ex: *thresholds* definidos); b) O alerta é registrado com status “em atenção”; c) Encaminhado automaticamente para avaliação (1.7). Se o processo não estiver implantado (considera-se o mínimo necessário): a) Técnico identifica visualmente, por observação periódica, que há um comportamento fora do normal; b) Registra manualmente o evento como “alerta” em planilha ou e-mail interno; c) Encaminha a informação ao responsável técnico para análise de impacto (1.7), mesmo sem ferramenta de correlação automática.
Recursos:
Se implantado: a) ferramenta com regras de limiar (*thresholds*), dashboards e notificação automática. Se não implantado (considera-se o mínimo necessário): a) observação direta do comportamento dos ativos, controle em planilha (ex: excel).
Entrada:
Evento classificado como “alerta” na correlação (1.2), ou identificado visualmente.
Ação:
Encaminhar o evento para análise detalhada de impacto e urgência (1.7).
Saída:
Evento em avaliação técnica na etapa 1.7.
1.5 Exceção

Descrição:
Evento classificado como exceção representa uma falha ativa, comportamento anômalo severo ou violação crítica dos parâmetros operacionais. Exige análise e resposta técnica imediata, pois pode comprometer a disponibilidade ou integridade dos serviços de TI.
Atores Envolvidos:
- Sistema de Monitoramento. - Analista de TI. - Coordenador Técnico ou Supervisor de TI.
Etapas:
Se o processo estiver implantado: a) O sistema de monitoramento aplica regras críticas de detecção de falhas (ex.: serviço parado, perda de pacote crítica, ausência de resposta); b) Evento é automaticamente classificado como exceção; c) Encaminhado para a etapa (1.7). Se o processo não estiver implantado (considera-se o mínimo necessário): a) Técnico identifica a falha por observação direta (ex: alerta visual no painel, usuários reclamando, perda de comunicação); b) Registra manualmente o evento como exceção em planilha, e-mail ou sistema informal; c) Encaminha imediatamente para avaliação técnica (1.7), ainda que não exista um procedimento formal definido.
Recursos:
Se implantado: a) Ferramenta com regras de exceção e *trigger*s configurados, notificações automatizadas e integração com sistema de *tickets*. Se não implantado (considera-se o mínimo necessário): a) Percepção técnica de falha e registro manual (planilha, formulário ou e-mail).
Entrada:
Evento classificado como exceção após correlação (1.2) ou detecção direta de falha crítica/severa.
Ação:
Encaminhar imediatamente o evento para avaliação crítica de impacto e urgência (1.7).
Saída:
Evento sob avaliação técnica na etapa (1.7).
1.6 Registrar Evento para Histórico
Descrição:
Armazena eventos classificados como informativos ou solucionados, mantendo rastreabilidade, geração de relatório e histórico técnico.
Atores Envolvidos:
- Sistema de Monitoramento. - Analista de TI.
Etapas:
Se o processo estiver implantado: a) Registro automático no banco de dados da ferramenta; b) Geração de relatório. Se o processo não estiver implantado (considera-se o mínimo necessário): a) Registro manual em planilha ou sistema básico;

b) Registro de status “sem impacto".

Recursos:

a) Sistema de monitoramento ou planilha institucional.

b) Estrutura de pastas de histórico.

Entrada:

Evento informativo (1.3).

Evento solucionado (1.22).

Ação:

Atualizar o relatório de eventos.

Registrar e arquivar o evento.

Saída:

Evento registrado.

Processo finalizado para eventos informativos e solucionados.

1.7 Aplicar Matriz de Criticidade

Descrição:

Esta etapa tem como objetivo avaliar o nível de impacto (sobre o serviço, usuários ou negócio) e a urgência (tempo necessário de resposta) do evento identificado com base na Matriz de Criticidade. O resultado define a prioridade de tratamento (baixa, média ou alta), orientando a resposta técnica adequada, cruzando os níveis de impacto e urgência do evento.

Atores Envolvidos:

- Analista de TI.
- Coordenador Técnico ou Supervisor de TI.

Etapas:

Se o processo estiver implantado:

a) Identificação do impacto: número de usuários afetados, criticidade do serviço, impacto financeiro ou legal;

b) Avaliação da urgência: tempo aceitável de resposta ou recuperação;

c) Aplicação formal da Matriz de Criticidade (Impacto × Urgência);

d) Registro automático da prioridade (baixa, média ou alta) no sistema.

Se o processo não estiver implantado, (considera-se o mínimo necessário):

a) Análise empírica da situação (ex.: serviço crítico fora do ar = alto impacto);

b) Avaliação baseada na experiência da equipe;

c) Uso de matriz simplificada (ex: papel, planilha excel, legenda de semáforo);

d) Registro da classificação em planilha, e-mail ou formulário não estruturado.

Recursos:

Se implantado:

a) Matriz formal de Criticidade validada.

b) Critérios institucionais de impacto e urgência.

c) SLA e Inventário com níveis de criticidade atribuídos.

d) Sistema de monitoramento com módulo de priorização automática.

Se não implantado (considera-se o mínimo necessário):

a) Tabela simplificada de referência (ex: matriz em papel ou digital básica).

b) Experiência técnica acumulada da equipe.

c) Planilhas para controle manual de prioridades.

Entrada:
Evento classificado como Alerta ou Exceção nas etapas anteriores.
Ação:
Aplicar a Matriz de Criticidade para definição da prioridade do evento.
Saída:
Evento priorizado com base na classificação obtida (baixa, média ou alta). Direcionamento para o fluxo correspondente (ex: tratamento direto, abertura de incidente, registro apenas, etc).
1.8 Classificar e Direcionar Tratamento
Descrição:
Após a aplicação da Matriz de Criticidade na etapa (1.7), esta fase registra e valida a classificação atribuída (baixa, média ou alta prioridade), direcionando o evento para o tratamento adequado: registro simples, incidente ou problema.
Atores Envolvidos:
- Analista de TI. - Coordenador Técnico ou Supervisor de TI.
Etapas:
Se o processo estiver implantado: a) Sistema valida a classificação atribuída na Matriz de Criticidade. b) Evento é automaticamente encaminhado conforme a prioridade: - Baixa: apenas registro; - Média: abertura de incidente; - Alta: abertura de incidente crítico ou escalonamento para problema. c) Classificação e decisão são salvas no histórico de eventos para consulta e auditoria (Atualizar Relatório de Eventos). Se o processo não estiver implantado (considera-se o mínimo necessário): a) Técnico registra a decisão de prioridade manualmente; b) Usa-se regra simples de decisão (ex: legenda de semáforo, fluxograma impresso); c) Encaminha manualmente para a tratativa correspondente (via e-mail, formulário ou verbalmente); d) Anota-se a decisão em planilha ou documento informal.
Recursos:
Se implantado: a) Sistema de gerenciamento de eventos com campos de criticidade. b) Regras de encaminhamento automatizado. c) Base de dados com histórico de classificações. Se o processo não estiver implantado (considera-se o mínimo necessário): a) Planilhas ou formulários simples para anotação. b) Roteiros visuais de decisão (fluxograma impresso ou cartaz). c) Conhecimento empírico da equipe.
Entrada:
Evento priorizado na etapa (1.7) (classificação obtida com base na Matriz de Criticidade).
Ação:
Confirmar e registrar a prioridade atribuída, decidindo o tratamento adequado.
Saída:
Evento classificado conforme resultado da Matriz de Criticidade: (Baixa, Média ou Alta).

Atualiza o Relatório de Eventos.

1.9 Baixa

Descrição:

Eventos classificados como baixa prioridade após a aplicação da Matriz de Criticidade são aqueles que apresentam um risco mínimo ou impacto limitado. Embora tenham sido inicialmente identificados como "Alertas" (1.4), após análise detalhada, podem não requerer ação imediata. Cabe, nesta etapa, avaliar se o evento demanda uma ação futura (abertura de chamado) ou se basta o registro para fins históricos.

Atores Envolvidos:

- Analista de TI.
- Coordenador Técnico ou Supervisor de TI.

Etapas:

Se o processo estiver implantado:

a) Avaliar se o evento com baixa prioridade exige acompanhamento ou intervenção posterior, baseado em critérios técnicos ou históricos anteriores;

b) Caso necessite acompanhamento ou ação futura, abrir chamado no sistema ITSM (encaminhar para etapa 1.15);

c) Caso contrário, registrar o evento apenas no histórico (encaminhar para etapa 1.6).

Se o processo não estiver implantado (Considera-se o mínimo necessário):

a) Técnico avalia manualmente o evento, considerando experiência e contexto;

b) Decide pela abertura manual de chamado (registro simples em planilha ou envio por e-mail);

c) Se não houver necessidade futura, registra-se informalmente para controle de histórico.

Recursos:

Se implantado:

a) Ferramenta ITSM integrada (ex: GLPI, Ocomon).

b) Procedimento institucional para classificação e abertura de chamados.

c) Base de conhecimento técnica e histórica.

Se o processo não estiver implantado (Considera-se o mínimo necessário):

a) Planilhas para controle manual de chamados ou históricos.

b) Formulários simples ou comunicação interna via e-mail.

Entrada:

Evento classificado como "Baixa Prioridade" na etapa 1.8 (aplicação da Matriz de Criticidade).

Ação:

Avaliar tecnicamente se o evento requer abertura de chamado técnico para acompanhamento ou se é suficiente apenas o registro para histórico (1.6).

Exemplos práticos:

Baixa prioridade com necessidade de abrir chamado:

Ex: Alerta recorrente de uso moderado da memória RAM em um servidor, que não afeta a operação atual, mas exige monitoramento preventivo ou ação futura.

Baixa prioridade sem necessidade de abrir chamado:

Ex: Alerta pontual de pico momentâneo em uso de rede ou CPU, já normalizado e sem tendência de repetição. Não exige intervenção futura, porém deve ficar registrado por rastreabilidade e auditoria.

Saída:

Evento encaminhado para abertura formal de chamado (1.12), quando necessário acompanhamento futuro ou ação preventiva ou encaminhado para registro no histórico (1.6), caso o evento não tenha necessidade de monitoramento posterior ou intervenção.
1.10 Média
Descrição:
Eventos classificados com média prioridade indicam uma condição técnica relevante que precisa de intervenção estruturada, mas sem urgência crítica imediata. Antes de abrir chamado, o evento deve ser avaliado para categorização clara como incidente (impacto operacional atual) ou problema (condição recorrente ou estrutural). Somente após esta definição é que ocorre a abertura formal do chamado (1.15).
Atores Envolvidos:
- Analista TI. - Coordenador Técnico ou responsável pela análise de incidentes/problemas.
Etapas:
Se o processo estiver implantado: a) Avaliação técnica do evento para identificar se representa um incidente (falha atual ou interrupção de serviço) ou problema (falha recorrente, causa raiz desconhecida ou estrutural); b) Definição e categorização clara do evento (Incidente ou Problema); c) Encaminhamento do evento categorizado para abertura formal de chamado no sistema ITSM (1.15). Se o processo não estiver implantado (considera-se o mínimo necessário): a) Avaliação empírica do evento com base na experiência da equipe técnica; b) Definição informal se o evento é incidente (necessidade imediata) ou problema (recorrente ou estrutural); c) Registro manual ou encaminhamento por e-mail para formalizar abertura de chamado (1.15).
Recursos:
Se o processo estiver implantado: a) Procedimento formal de categorização incidente/problema. b) Base de Conhecimento institucional. c) Ferramenta ITSM (ex: GLPI, Ocomon ou similar). Se o processo não estiver implantado (considera-se o mínimo necessário): a) Conhecimento baseado na experiência dos técnicos envolvidos. b) Registro manual em planilhas ou documentos informais.
Entrada:
Evento classificado como média prioridade (1.8).
Ação:
Avaliar e categorizar o evento como incidente ou problema antes da abertura formal do chamado.
Saída:
Evento categorizado claramente como incidente ou problema; Encaminhado para etapa (1.15) - Abrir Chamado ou Solicitação de Suporte.
1.11 Alta
Descrição:
Eventos classificados com alta prioridade são incidentes ou exceções críticas, com impacto severo ou potencial risco significativo à continuidade operacional. Exigem tratamento urgente, podendo requerer ação imediata (contorno) e posteriormente a análise detalhada da violação (causa-raiz).

Atores Envolvidos:
- Analista TI. - Coordenador Técnico ou responsável pela análise de incidentes/problemas.
Etapas:
Se o processo estiver implantado: a) Encaminha diretamente para ação de contorno imediata (1.16). Se o processo não estiver implantado (considera-se o mínimo necessário): a) Aciona equipe técnica diretamente para ação emergencial informal; b) Avaliação rápida e registro simplificado para posterior análise detalhada.
Recursos:
Se o processo estiver implantado: a) Sistema ITSM, ferramenta de registro e análise, base de conhecimento. Se o processo não estiver implantado (considera-se o mínimo necessário): a) Comunicação direta (telefone, e-mail), registro manual.
Entrada:
Evento classificado como alta prioridade (1.8).
Ação:
Direcionar para contorno imediato e análise técnica posterior.
Saída:
Encaminhamento para etapa (1.16) - Encaminhar para Ação de Contorno.
1.12 Categorizar Evento
Descrição:
Esta atividade consiste na categorização do evento previamente classificado como relevante (criticidade média, alta ou muito alta), devendo encaminhar para 1.15 e encaminhamento para 1.13 ou 1.14.
Atores Envolvidos:
-Suporte (Técnico ou Analista): valida ou ajusta a categoria sugerida. -Gestor de TI ou Coordenador de Incidentes: em casos críticos, pode redefinir a categoria ou encaminhar para tratamento específico (problemas ou mudanças).
Etapas:
Se o processo estiver implantado: a) Recepção do evento classificado (via motor Fuzzy). b) Registro do chamado no GLPI com categoria padrão (pré-configurada por tipo de *trigger*, host ou criticidade). c) Confirmação da categorização e continuidade no fluxo (ex: encaminhar para gerenciamento de incidentes ou problemas). d) Armazenamento da categoria no banco de dados do chamado. Se o processo não estiver implantado (considera-se o mínimo necessário): a) Analista recebe notificação de evento relevante (por e-mail, monitoramento ou manualmente). b) Abertura manual do chamado no GLPI (ou ferramenta equivalente). c) Analista analisa o evento e define a categoria manualmente, com base em: i) Descrição do evento ii) Equipamento afetado iii) Serviço impactado d) Categoria é registrada no chamado manualmente.
Recursos:

Se o processo estiver implantado: a) GLPI com regras de negócios ativas para categorização automática. b) Integração GLPI com Motor Fuzzy via API REST (Python). c) Tabela de mapeamento entre *trigger*s/hosts e categorias. d) Interface web do GLPI para validação por analistas. e) Logs de auditoria habilitados. f) Base de conhecimento integrada (opcional). Se o processo não estiver implantado (considera-se o mínimo necessário): a) Interface administrativa do GLPI ou sistema de ITSM equivalente. b) Equipe técnica treinada em classificação de eventos. c) Guia interno ou planilha de correspondência entre tipos de evento e categorias. d) Procedimentos operacionais padrão (POP) para categorização.
Entrada:
Evento validado pelo motor Fuzzy com criticidade e dados do evento.
Ação:
Executar categorização automática preliminar com base em regras configuradas (ex: por grupo de ativos, serviço impactado, criticidade). Apresentar categoria ao analista de suporte para validação ou correção. Atualizar a categoria no chamado e encaminhar o item para o processo de resolução adequado, conforme a classificação (incidente ou problema)
Saída:
Chamado no GLPI com categoria definida (ex: Rede - Link externo / Hardware - Switch). Direcionamento do fluxo para o item correspondente: a) Incidente: item 1.13; b) Problema: item 1.14.
1.13 Encaminhar Gerenciamento de Incidentes
Descrição:
Esta etapa é acionada sempre que o evento monitorado requer acompanhamento técnico formal, seja por se tratar de um incidente em andamento, um evento contornado, ou uma solicitação de suporte relacionada. A partir deste ponto, o evento passa a ser tratado conforme o fluxo de Gerenciamento de Incidentes ou o processo de atendimento via Service Desk, conforme a estrutura da instituição.
Atores Envolvidos:
- Analista TI. - Coordenador Técnico ou responsável pela análise de incidentes/problemas.
Etapas:
Se o processo estiver implantado: a) Atender o chamado referente ao incidente no sistema ITSM. b) Registro de todos os dados relevantes: IC, prioridade, sintomas, logs, usuário impactado. c) Encaminhamento para a fila correta de atendimento. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Registro do chamado de forma simplificada (formulário, e-mail, planilha). b) Encaminhamento para responsável técnico por meio informal. c) Controle e atualização do atendimento por métodos alternativos.

Recursos:
Se o processo estiver implantado: a) Sistema ITSM (ex: GLPI, OTRS, etc.); b) Catálogo de Serviços e Matriz de Priorização. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Canal informal de abertura (e-mail, WhatsApp institucional, planilha); b) Designação manual de responsáveis.
Entrada:
Evento que requer atendimento técnico formal (ex: evento contornado ou incidente ativo).
Ação:
Iniciar tratativa do incidente em fluxo próprio.
Saída:
Evento tratado no fluxo de Gerenciamento de Incidentes.
1.14 Encaminhar Gerenciamento de Problemas
Descrição:
Quando um evento é contornado, mas não possui uma solução definitiva, ele deve ser formalmente encaminhado para o processo de Gerenciamento de Problemas. Esse processo visa identificar a causa raiz da falha e propor ações corretivas estruturais. A partir deste ponto, o evento deixa o fluxo de monitoramento e passa a ser tratado conforme o fluxo específico de Problemas, conforme definido na estrutura organizacional da TI.
Atores Envolvidos:
- Analista TI. - Coordenador Técnico ou responsável pela análise de incidentes/problemas.
Etapas:
Se o processo estiver implantado: a) Atender o chamado referente ao problema no sistema ITSM. b) Iniciar a análise da causa raiz. c) Associar o problema a incidentes recorrentes (se houver). d) Propor ações corretivas definitivas. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Registrar o problema de forma simplificada (planilha, e-mail ou documento informal). b) Designar responsável técnico. c) Conduzir análise ad hoc com base na experiência. d) Monitorar evolução do caso manualmente.
Recursos:
Se o processo estiver implantado: a) Módulo de Gerenciamento de Problemas do ITSM b) Base de Conhecimento c) Histórico técnico de incidentes Se o processo não estiver implantado (considera-se o mínimo desejável): a) Controle local (planilhas ou arquivos) b) *Logs*, registros manuais e conhecimento técnico.
Entrada:
Evento classificado como “contornado” (etapa 1.22).

Ação:
Iniciar tratativa do problema em fluxo próprio.
Saída:
Evento tratado no fluxo de Gerenciamento de Problemas.
1.15 Abrir Chamado ou Solicitação de Suporte
Descrição:
Esta atividade tem por objetivo registrar formalmente um chamado ou uma solicitação de suporte no sistema de ITSM (ex: GLPI), com base nas informações do evento classificado e categorizado. A abertura do chamado permite o tratamento estruturado, rastreável e baseado em SLA, conforme práticas da ITIL 4.
Atores Envolvidos:
-Sistema GLPI (automatizado): executa categorização preliminar com base em parâmetros do evento (origem, criticidade, host). -Suporte (Técnico ou Analista): valida ou ajusta a categoria sugerida. -Gestor de TI ou Coordenador de Incidentes: em casos críticos, pode redefinir a categoria ou encaminhar para tratamento específico (problemas ou mudanças).
Etapas:
Se o processo estiver implantado: a) A decisão lógica (baseada na criticidade + tipo de evento) determina se deve ser aberto um chamado. b) Motor Fuzzy envia, via *webhook*, os dados completos ao GLPI (ex: ID do evento, Nome do *host*, *Trigger*, Criticidade Fuzzy, Data/hora). c) Script Python autentica na API do GLPI e realiza a abertura automática do chamado com: (ex: Título, descrição e categoria pré-definidos, Urgência e impacto baseados na matriz Fuzzy, Número do chamado). d) Chamado segue automaticamente para análise, tratamento ou apenas registro para histórico (item 1.16 ou 1.13, conforme a natureza do evento). Se o processo não estiver implantado (considera-se o mínimo desejável): a) Analista técnico ou operador identifica a necessidade de registrar um evento como chamado. b) Abertura manual do chamado via interface do sistema GLPI ou ferramenta equivalente. c) Preenchimento manual dos campos: (ex: Título, descrição do problema, data e hora, criticidade estimada (com base na experiência do analista), categoria e tipo de chamado (incidente, requisição etc.). d) Registro da abertura e geração do número do chamado. e) Encaminhamento do chamado para tratamento técnico (item 1.16 ou 1.13). f) Notificação ao solicitante (se houver) e início do controle por SLA.
Recursos:
Se o processo estiver implantado: a) Zabbix, Motor Fuzzy em Python e GLPI com *webhook* e API REST configurados. b) Script Python de integração (com tratamento de erro e resposta) c) Motor Fuzzy com script função "criar_chamado_glpi" d) Logs e controle de duplicidade e) Base de conhecimento consultável (opcional) f) Matriz de criticidade com impacto, urgência, criticidade, host. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Dados do ativo;

b) Ferramenta ITSM ou controle manual (planilha) para abertura de chamados

c) Procedimentos operacionais padrão (POP);

d) Matriz de criticidade mesmo que básica;

e) Manual de categorização.

Entrada:

Se implementado:

Evento classificado conforme criticidade

Dados recebidos: (ex: *event_id*, *event_name, host_name e host_ip*, *trigger*, impacto, urgência e criticidade, Fuzzy)

Regras de decisão aplicadas (ex: abrir chamado se ativo cadastrado no mapa de decisão)

Parâmetros do mapa de decisão (YAML) carregados.

Ação:

Motor Fuzzy executa validação se evento já foi processado, se não foi, prepara e envia um *payload* via requisição POST para o *endpoint* da API REST do GLPI, Script Python autentica, cria sessão e envia os dados do chamado:

Título, descrição, tipo, categoria, prioridade, grupo técnico. GLPI registra o chamado com status inicial.

Número do chamado é retornado e armazenado no log de eventos processados.

Saída:

Chamado registrado automaticamente no GLPI, com número único.

Campos preenchidos: título, descrição, criticidade, categoria, data/hora, equipe responsável.

Evento marcado como "processado" no sistema Fuzzy (evita duplicidade).

Geração de log local ou resposta JSON confirmando sucesso.

Encaminhamento automático do chamado para tratamento (item 1.13, 1.14 ou 1.16).

1.16 Encaminhar para Ação de Contorno

Descrição:

Aplicação rápida e imediata de medidas provisórias para reduzir ou neutralizar o impacto do evento até a solução definitiva.

Atores Envolvidos:

- Analista TI.

- Coordenador Técnico ou responsável pela análise de incidentes/problemas.

Etapas:

Se o processo estiver implantado:

a) Executar procedimentos formais de contorno descritos na Base de Conhecimento.

Se o processo não estiver implantado (considera-se o mínimo desejável):

a) Aplicação imediata e informal de medidas técnicas com base na experiência da equipe, sem documentação formal inicial.

Recursos:

Se o processo estiver implantado:

a) Base de Conhecimento estruturada.

b) Procedimentos formais de contorno.

Se o processo não estiver implantado (considera-se o mínimo desejável):

a) Conhecimento empírico da equipe técnica.

Entrada:

Evento crítico (Alta prioridade).

Ação:

Executar medida provisória imediata.

Saída:

Evento encaminhado para análise detalhada (1.17).
1.17 Analisar Violação (exceção)
Descrição:
Analisa e identifica as causas e impactos da exceção ou violação.
Atores Envolvidos:
- Analista de TI. - Coordenador Técnico ou responsável pela análise de incidentes/problemas.
Etapas:
Se o processo estiver implantado: a) Avaliação formal detalhada (logs, histórico, métricas); b) Elaboração estruturada de relatório. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Avaliação empírica e informal baseada em registros mínimos (logs básicos, relatos verbais); b) Registro simplificado (planilha, e-mail ou relatório informal).
Recursos:
Se o processo estiver implantado: a) Sistema automatizado de monitoramento e análise. b) Templates formais de relatórios. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Documentação manual (ex: planilha excel, e-mail, documento Word).
Entrada:
Evento após ação de contorno (1.16).
Ação:
Gerar relatório detalhado do evento.
Saída:
Dados encaminhados para (1.18).
1.18 Definir Ação a ser Tomada
Descrição:
Escolhe as ações corretivas com base na análise anterior, considerando necessidade de autorização superior.
Atores Envolvidos:
- Analista TI. - Coordenador Técnico ou responsável pela análise de incidentes/problemas.
Etapas:
Se o processo estiver implantado: a) Consultar Inventário e Base de Conhecimento formal; b) Elaborar plano formal de ação corretiva; c) Avaliar formalmente necessidade de autorização superior. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Avaliação informal com base em conhecimento técnico empírico; b) Registro simples das ações propostas; c) Decisão empírica sobre autorização superior.
Recursos:

Se o processo estiver implantado: a) Base de Conhecimento institucional. b) Inventário atualizado. c) Plano de Ação formal. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Registro simples (planilha ou documento informal). b) Experiência empírica da equipe.
Entrada:
Relatório do evento (1.17), Inventário e Base de conhecimento.
Ação:
Definir ações corretivas necessárias.
Saída:
Decisão sobre necessidade de autorização superior: Caso sim: encaminha para etapa (1.19); Caso não: Encaminha para etapa (1.20).
1.19 Aguardar Autorização Superior
Descrição:
Obtenção formal ou informal de autorização superior antes da execução de ações corretivas críticas.
Atores Envolvidos:
- Gestor Superior ou Diretor de TI.
Etapas:
Se o processo estiver implantado: a) Solicitação formal documentada; b) Recebimento de autorização documentada. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Solicitação informal por telefone, e-mail ou reunião rápida; b) Registro mínimo da aprovação (e-mail ou verbalmente anotado).
Recursos:
Se o processo estiver implantado: a) Documentação formal (sistema de workflow ou e-mail institucional). Se o processo não estiver implantado (considera-se o mínimo desejável): b) Comunicação informal (telefone, WhatsApp, e-mail).
Entrada:
Decisão da etapa (1.18).
Ação:
Conceder autorização.
Saída:
Autorização obtida, encaminha para etapa (1.20).
1.20 Executar Ação
Descrição:
Execução prática das ações corretivas definidas.
Atores Envolvidos:

- Analista TI. - Coordenador Técnico ou responsável pela análise de incidentes/problemas.
Etapas:
Se o processo estiver implantado: a) Executar plano formal de ação registrado; b) Verificar formalmente restabelecimento da operação. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Execução direta com base no conhecimento da equipe; b) Avaliação empírica de retorno operacional.
Recursos:
Se o processo estiver implantado: a) Plano formal documentado (ferramenta ITSM ou documento estruturado). Se o processo não estiver implantado (considera-se o mínimo desejável): b) Registro simplificado (planilha, documento informal).
Entrada:
Plano de Ação, autorização (se aplicável, 1.19).
Ação:
Executar ações corretivas definidas.
Saída:
Decisão sobre restabelecimento operacional do IC ou serviço: Caso sim: encaminha para etapa (1.21); Caso não: retorna para etapa (1.18).
1.21 Atualizar Base de Conhecimento
Descrição:
Atualiza as informações sobre as soluções adotadas para análise futura.
Atores Envolvidos:
- Analista TI. - Coordenador Técnico ou responsável pela análise de incidentes/problemas.
Etapas:
Se o processo estiver implantado: a) Registrar formalmente solução aplicada na Base de Conhecimento institucional. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Registro simples em documentos locais ou planilhas.
Recursos:
Se o processo estiver implantado: a) Base de conhecimento estruturada. Se o processo não estiver implantado (considera-se o mínimo desejável): b) Planilha ou documento local.
Entrada:
Ação executada com sucesso (1.20).
Ação:
Registrar solução adotada.
Saída:

Base atualizada e encaminha para a etapa (1.22).
1.22 Comunicar Partes Interessadas
Descrição:
Realiza comunicação clara e direta às partes interessadas sobre o incidente ou problema e sua resolução.
Atores Envolvidos:
- Analista TI. - Coordenador Técnico ou responsável pela análise de incidentes/problemas.
Etapas:
Se o processo estiver implantado: a) Comunicação formal e estruturada via e-mail institucional ou sistema ITSM. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Comunicação informal por telefone, WhatsApp ou e-mail simples.
Recursos:
Se o processo estiver implantado: a) Ferramenta formal de comunicação institucional. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Canais informais (telefone, e-mail simples, WhatsApp).
Entrada:
Solução registrada e Base atualizada (1.21).
Ação:
Comunicar resultado do tratamento.
Saída:
Avaliação final: Caso solucionado: encaminha para registro histórico (1.6); Caso contornado (sem solução definitiva): encaminha simultaneamente para: a) Gerenciamento de Problemas (1.14); b) Abertura formal de chamado (1.15).

APÊNDICE B – ESPECIFICAÇÃO DA MGE MANUAL

2.1 Escolher Item de Configuração (IC)
Descrição:
Nesta etapa, o analista seleciona qual ativo de TI será monitorado. A escolha é baseada no inventário e no plano de monitoramento. Trata-se de um passo essencial para direcionar a coleta de dados e garantir que o foco do monitoramento esteja alinhado com os objetivos institucionais.
Atores Envolvidos:
- Analista de infraestrutura de TI. - Técnico de Redes. - Funcionário designado ou responsável pelo Monitoramento de Serviços de TI.
Etapas:
Se o processo estiver implantado: a) Acessar o banco de dados de inventário; b) Verificar o Plano de Monitoramento; c) Selecionar o ativo (IC) mais crítico ou relevante. Se o processo não estiver implantado (considera-se o mínimo necessário): a) Consultar planilha ou lista básica com os ativos conhecidos; b) Escolher manualmente o ativo a ser acompanhado; c) Registrar a escolha em documento simples ou anotações internas.
Recursos:
Se o processo estiver implantado: a) Inventário de ICs (mesmo que planilha ou similar). b) Plano de Monitoramento. c) Terminal com acesso a ferramenta de Monitoramento. d) Ferramenta de Monitoramento (ex: Zabbix, iTop, Log Analyzer ou similar). Se o processo não estiver implantado (considera-se o mínimo necessário): a) Lista básica (mesmo que não atualizada) com nome dos servidores, equipamentos ou links (ativos). b) Alguma identificação mínima do ativo (nome, IP ou localidade).
Entrada:
Processo iniciado. Acesso ao inventário/planilha e ao plano de monitoração.
Ação:
Selecionar, com base nos dados disponíveis, o item de configuração que será monitorado.
Saída:
Item de Configuração (IC) selecionado. Atividade encaminhada para coleta de dados (2.2).
2.2 Coletar Dados
Descrição:
Esta etapa consiste na coleta de dados operacionais e históricos do ativo selecionado, como logs, métricas, status ou alertas anteriores. O objetivo é obter evidências para análise e tomada de decisão na próxima etapa do fluxo.
Atores Envolvidos:

- Analista de infraestrutura de TI.
- Técnico de Redes.
- Funcionário designado ou responsável pelo Monitoramento de Serviços de TI.

Etapas:

Se o processo estiver implantado:

a) Acessar a ferramenta de monitoramento (ex: Zabbix, GLPI, Log Analyzer ou similar);

b) Extrair logs, gráficos, alertas ou indicadores de desempenho.

Se o processo não estiver implantado (considera-se o mínimo necessário):

a) Acessar o ativo diretamente (via SSH, RDP ou painel do equipamento);

b) Copiar manualmente logs ou prints;

c) Registrar informações relevantes em planilha ou arquivo local.

Recursos:

Se o processo estiver implantado:

a) Ferramenta de monitoramento configurada (Zabbix, itop, Log Analyzer ou similar).

b) Dashboard técnico.

Se não estiver implantado (considera-se o mínimo necessário):

a) Acesso ao ativo (servidor, switch, etc.).

b) Conhecimento básico sobre onde localizar os dados.

Entrada:

IC selecionado na etapa 2.1.

Acesso autorizado ao ativo.

Ação:

Coletar dados operacionais relevantes do IC.

Saída:

Conjunto de dados coletados (logs, métricas, status);

Direcionamento para análise técnica (2.3).

2.3 Analisar Dados

Descrição:

Esta etapa visa interpretar os dados coletados, com foco na identificação de anomalias, falhas, degradação ou instabilidades. A partir dessa análise, o evento será classificado como incidente, problema ou condição normal, direcionando o fluxo apropriadamente.

Atores Envolvidos:

- Analista de infraestrutura de TI.
- Técnico de Redes.
- Funcionário designado ou responsável pelo Monitoramento de Serviços de TI.

Etapas:

Se o processo estiver implantado:

a) Avaliar os dados utilizando critérios do Plano de Monitoramento;

b) Identificar padrões de falha ou degradação;

c) Elaborar relatório de atividade técnica;

d) Classificar o evento.

Se o processo não estiver implantado (considera-se o mínimo necessário):

a) Revisar manualmente os logs e prints coletados;

b) Aplicar julgamento técnico com base na experiência;

c) Registrar a análise em planilha ou e-mail;

d) Classificar o evento com base na criticidade observada (mesmo que informalmente).

Recursos:

Se o processo estiver implantado:

- Ferramenta de análise técnica.
- Template de relatório de atividade.
- Histórico de eventos anteriores.

Se não estiver implantado (considera-se o mínimo necessário):

- Capacidade técnica para interpretar os dados.
- Modelo básico de registro da análise (documento Word, planilha, e-mail).

Entrada:

- Dados coletados (2.2).
- Plano de Monitoramento (se houver).
- Conhecimento técnico da equipe.

Ação:

Realizar análise técnica, identificar possíveis causas e classificar o evento conforme impacto e recorrência.

Saída:

- Relatório de atividade produzido;
- Decisão:

a) Se incidente: Encaminhar para 2.4 - Gerenciamento de Incidente;

b) Se problema: Encaminhar para 2.5 - Gerenciamento de Problema;

c) Se normal: Encerrar o processo.

2.4 Gerenciamento de Incidente

Descrição:

Esta etapa é acionada quando, após análise técnica dos dados coletados (etapa 2.3), o evento é classificado como incidente, ou seja, uma interrupção ou degradação inesperada na qualidade de um serviço de TI que afeta diretamente a operação. O objetivo é restaurar o serviço o mais rápido possível, minimizando o impacto no negócio.

Atores Envolvidos:

- Analista de infraestrutura de TI.
- Técnico de Redes.
- Funcionário designado ou responsável pelo Monitoramento de Serviços de TI.

Etapas:

Se o processo de Gerenciamento de Incidentes estiver implantado:

a) Registrar o incidente no sistema de chamados.

b) Classificar e categorizar o incidente.

c) Acionar os responsáveis pela resolução.

d) Acompanhar a execução da ação corretiva.

e) Atualizar o status do incidente até a resolução e encerramento.

Se o processo não estiver implantado (considera-se o mínimo desejável):

a) Registrar o incidente em planilha de controle ou e-mail.

b) Descrever brevemente o impacto observado e o ativo afetado.

c) Encaminhar o caso à equipe técnica com prioridade definida de forma colaborativa.

d) Documentar a solução aplicada e o tempo de resolução.

e) Arquivar o registro como insumo para implantação futura do processo.

Recursos:

Se o processo estiver implantado:

a) Sistema de chamados ou ITSM (ex.: GLPI, iTop, Ocomon ou similar).

b) Base de Conhecimento.

c) Comunicação integrada com a equipe técnica.

Se o processo não estiver implantado (considera-se o mínimo desejável):

a) Planilha de controle (como ex: excel).

b) E-mail institucional.

c) Histórico manual de ocorrências.

Entrada:

Evento classificado como incidente na etapa 2.3.

Indício de falha com impacto direto à operação do serviço de TI ou do usuário final.

Ação:

Se o processo estiver implantado:

Ativar o processo de Gerenciamento de Incidentes, registrando e acompanhando a tratativa conforme o fluxo definido.

Se o processo não estiver implantado (considera-se o mínimo desejável):

Realizar atendimento técnico com registro manual e priorização baseada no impacto observado.

Saída:

Se o processo estiver implantado:

a) Incidente resolvido com registro formal no sistema.

b) Atualização da Base de Conhecimento (se aplicável).

Se o processo não estiver implantado (considera-se o mínimo desejável):

a) Serviço restaurado.

b) Registro do incidente armazenado para fins históricos e melhoria contínua futura.

2.5 Gerenciamento de Problema

Descrição:

Esta etapa é acionada quando, após análise técnica dos dados coletados (etapa 2.3), o evento é classificado como problema, ou seja, está relacionado a uma causa raiz não imediata, é recorrente ou revela falhas estruturais no ambiente de TI. O objetivo é iniciar uma investigação mais aprofundada para identificar e eliminar a origem do problema.

Atores Envolvidos:

- Analista de infraestrutura de TI.
- Técnico de Redes.
- Funcionário designado ou responsável pelo Monitoramento de Serviços de TI.

Etapas:

Se o processo de Gerenciamento de Problemas estiver implantado:

a) Registrar o problema no sistema.

b) Iniciar análise da causa raiz.

c) Associar a incidentes anteriores (se houver).

d) Avaliar necessidade de ações corretivas estruturais.

Se o processo não estiver implantado (considera-se o mínimo de sejável):

a) Registrar a ocorrência em planilha ou sistema de controle provisório (como ex: GLPI ou similar).

b) Identificar possíveis causas com base na análise técnica da etapa 2.3. c) Manter histórico documental da recorrência (como ex: planilha excel ou similar). d) Encaminhar o caso para avaliação técnica ou gerencial "ad hoc" (mínimo comunicar as partes interessadas). e) Utilizar o registro como insumo para justificar a implantação progressiva do processo.
Recursos:
Se o processo estiver implantado: a) Sistema de registro de problemas (ex.: GLPI, iTop, Ocomon ou similar). b) Histórico técnico de eventos recorrentes. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Planilha de controle de ocorrências (ex: excel ou similar). b) Arquivos digitais contendo evidências (logs, prints, descrições técnicas). c) Comunicação por e-mail entre equipes técnicas para registro informal .
Entrada:
Evento classificado como problema na etapa 2.3. Situação com recorrência, instabilidade ou degradação sem causa conhecida.
Ação:
Se o processo estiver implantado: - Ativar o fluxo de Gerenciamento de Problemas conforme definido na estrutura organizacional. Se o processo não estiver implantado (considera-se o mínimo desejável): - Registrar o evento como "problema potencial" em controle local. - Realizar avaliação técnica inicial. - Consolidar informações para futura análise ou implantação do processo.
Saída:
Se o processo estiver implantado: - Evento transferido ao fluxo formal de tratamento de problemas. - Registro disponível para análise de causa raiz e planejamento de ações corretivas. Se o processo não estiver implantado (considera-se o mínimo desejável): - Ocorrência registrada e armazenada. - Subsídio para desenvolvimento futuro do catálogo de problemas e estruturação formal do processo.

APÊNDICE C – ESPECIFICAÇÃO DO PLANO DE MONITORAÇÃO

3.1 Rever Processo de Monitoramento
Descrição:
Esta etapa consiste na revisão periódica ou pontual do processo de Monitoramento e Gerenciamento de Eventos (MGE), com o objetivo de identificar pontos de melhoria, desvio de escopo ou necessidade de atualização. Trata-se de uma etapa de diagnóstico técnico-processual.
Atores Envolvidos:
- Gestor de TI. - Analista responsável pelo MGE. - Auditor interno ou consultor (se aplicável). - Analista de infraestrutura de TI.
Etapas:
Se o processo estiver implantado: a) Reunir evidências do funcionamento do processo MGE; b) Revisar indicadores, registros e fluxos BPMN; c) Identificar lacunas, gargalos ou desvios. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Realizar entrevistas com a equipe técnica; b) Verificar se há algum fluxo, ainda que informal, de tratamento de eventos; c) Registrar observações em documento simples.
Recursos:
Se o processo estiver implantado: a) Documento oficial do Processo de MGE. b) Histórico de eventos monitorados (relatório de eventos). c) Indicadores ou dashboards operacionais. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Acesso aos registros manuais ou sistemas utilizados para eventos. b) Participação da equipe envolvida.
Entrada:
Processo de MGE vigente (Plano de Monitoração), sendo ele formal ou informal. Dados do Relatório de Eventos.
Ação:
Analisar a efetividade do processo atual, correlacionando com o relatório contendo o histórico de eventos e documentar oportunidades de melhoria.
Saída:
Diagnóstico técnico processual consolidado. Encaminhamento para etapa 3.2 (Análise e Proposição de Melhorias).
3.2 Analisar e Propor Melhorias
Descrição:

Nesta etapa, os dados levantados na revisão do processo são analisados, e são propostas ações de melhoria contínua que visem aprimorar o desempenho, a cobertura e a efetividade do monitoramento de eventos.
Atores Envolvidos:
- Gestor de TI. - Analista responsável pelo MGE. - Auditor interno ou consultor (se aplicável). - Analista de infraestrutura de TI.
Etapas:
Se o processo estiver implantado: a) Avaliar criticamente as informações geradas na etapa 3.1; b) Identificar causas e impactos dos pontos fracos observados; c) Formular, se houver, recomendações de melhoria viáveis; d) Consolidar essas recomendações em um Plano de Melhoria do MGE. Se o processo não estiver implantado (considera-se o mínimo necessário): a) Reunir a equipe técnica e/ou responsáveis operacionais para discutir as falhas ou dificuldades percebidas; b) Registrar informalmente as sugestões de melhoria, se houver, em um documento simples (ex: planilha, e-mail, ata de reunião); c) Priorizar ações que possam ser aplicadas com recursos existentes; d) Elaborar um plano mínimo de ação com prazos e responsáveis, mesmo que sem padronização formal; e) Utilizar esse documento como base para estruturar o processo de melhoria contínua no futuro.
Recursos:
Documento diagnóstico da etapa 3.1. Template de Plano de Melhoria (mesmo que simples). Conhecimento técnico e organizacional sobre o processo.
Entrada:
Diagnóstico do processo de MGE (3.1).
Ação:
Elaborar plano de ação com propostas de melhoria estruturadas para o processo de MGE, considerando a possibilidade de não haver alterações identificadas no ciclo de revisão.
Saída:
Caso haja proposta de alteração, o Plano de Melhoria do MGE é encaminhado para (3.3). Caso não sejam identificadas mudanças necessárias, o processo é encerrado.
3.3 Validar Alterações
Descrição:
A etapa de validação tem como objetivo aprovar (ou reprovar) as alterações propostas no Plano de Melhoria do MGE, com base em critérios técnicos, operacionais ou estratégicos. A decisão impacta diretamente a continuidade ou o retorno à etapa de revisão.
Atores Envolvidos:
- Gestor de TI. - Analista responsável pelo MGE. - Auditor interno ou consultor (se aplicável). - Analista de infraestrutura de TI.
Etapas:

Se o processo estiver implantado:

a) Analisar a viabilidade técnica e institucional das propostas;

b) Avaliar riscos e benefícios esperados;

c) Registrar a decisão (aprovado ou não aprovado);

d) Encaminhar para 3.4 em caso de aprovação;

e) Retornar para 3.1 em caso de necessidade de reavaliação.

Se o processo não estiver implantado (considera-se o mínimo necessário):

a) Submeter as propostas de melhoria à avaliação de um responsável técnico ou gestor da área (mesmo que informalmente);

b) Utilizar reuniões operacionais ou validação por e-mail como forma de decisão;

c) Registrar o aceite ou recusa das propostas em documento simples;

d) Caso aprovado, seguir para a execução das alterações (3.4); caso contrário, retornar à revisão (3.1), com os apontamentos do responsável.

Recursos:

Plano de Melhoria do MGE elaborado na etapa (3.2).

Critérios de aprovação (mesmo que mínimos).

Registro da decisão (e-mail, ata ou documento formal).

Entrada:

Plano de Melhoria do MGE.

Ação:

Validar (ou recusar) as alterações propostas com base em critérios técnicos e organizacionais.

Saída:

Se aprovado: encaminhamento para (3.4).

Se não aprovado: retorna para etapa (3.1), com recomendações para revisão das propostas.

3.4 Atualizar Plano de Monitoração

Descrição:

Etapa final do ciclo de melhoria, onde as alterações validadas são formalmente implementadas no processo de MGE. Esta atualização pode envolver mudanças em procedimentos, fluxos, ferramentas ou papéis e deve ser devidamente documentada e comunicada.

Atores Envolvidos:

- Gestor de TI.
- Analista responsável pelo MGE.
- Auditor interno ou consultor (se aplicável).
- Analista de infraestrutura de TI.

Etapas:

Se o processo estiver implantado:

a) Atualizar os documentos oficiais do processo MGE (fluxo BPMN, políticas, POPs, instruções de trabalho);

b) Registrar a nova versão do processo em sistema de gestão documental ou repositório interno;

c) Comunicar formalmente a equipe envolvida sobre as alterações;

d) Ajustar sistemas, ferramentas e responsabilidades conforme o plano aprovado;

e) Encerrar o ciclo de melhoria, registrando a execução no plano de ação.

Se o processo não estiver implantado (considera-se o mínimo necessário):

a) Atualizar manualmente os arquivos existentes (ex.: fluxogramas em PowerPoint, planilhas, documentos Word) com as mudanças acordadas;

b) Criar uma pasta compartilhada (em rede ou na nuvem) para armazenar a nova versão do fluxo ou dos procedimentos; c) Informar a equipe envolvida por e-mail, reunião interna ou mural físico, descrevendo as alterações realizadas; d) Registrar a data da mudança e manter os arquivos anteriores como versão histórica; e) Considerar essa ação como base inicial para implantar formalmente um sistema de controle de versões e melhoria contínua no futuro.
Recursos:
Versão anterior do Processo de MGE. Plano de Melhoria validado (2.3). Ferramentas de documentação e controle de versão (mesmo que planilha).
Entrada:
Plano de Melhoria do MGE validado.
Ação:
Executar a implementação das melhorias aprovadas no processo de MGE.
Saída:
Processo de MGE atualizado (formal ou provisório). Nova versão dos documentos em vigor. Registro da execução da melhoria. Encerramento do ciclo atual de melhoria.

APÊNDICE D – ESPECIFICAÇÃO DO PROCESSO MONITORAR

4.1 Monitorar
Descrição:
Esta etapa consiste na observação contínua ou periódica do comportamento dos ativos de TI (ICs), com base nos parâmetros definidos no Plano de Monitoramento e nas metas de desempenho estabelecidas no Acordo de Nível de Serviço (ANS). O objetivo é identificar variações, desvios ou comportamentos anômalos que possam gerar eventos.
Atores Envolvidos:
- Analista de Monitoramento - Equipe Técnica de Infraestrutura. - Coordenador de TI.
Etapas:
Se o processo estiver implantado: a) Configurar a ferramenta de monitoramento com base nos dados do inventário e parâmetros do ANS; b) Acompanhar dashboards e gráficos de forma ativa ou via alertas automáticos; c) Correlacionar dados com histórico de desempenho; d) Registrar alertas e condições anômalas detectadas. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Observar o comportamento dos ativos por meio de acessos diretos (via terminal, painel de equipamento ou software básico); b) Registrar manualmente qualquer anomalia percebida (ex: lentidão, falha de resposta); c) Utilizar controles básicos (como planilhas) para registrar tendências ou comportamentos anormais.
Recursos:
Se o processo estiver implantado: a) Ferramenta de monitoramento (ex: Zabbix, Itop, Log Analyzer ou similar). b) Plano de Monitoramento formalizado. c) Acordo de Nível de Serviço (ANS) vigente com parâmetros técnicos definidos. d) Histórico técnico de desempenho anterior. Se o processo não estiver implantado (considera-se o mínimo necessário): a) Acesso contínuo ou recorrente ao ativo monitorado. b) Alguma forma de registrar o comportamento observado (ex: planilha, print, relatório informal).
Entrada:
Acordo de Nível de Serviço (ANS). Dados do Inventário de ICs. Parâmetros definidos no Plano de Monitoramento. Dados históricos ou anteriores do ativo (se disponíveis) .
Ação:
Acompanhar o comportamento do IC com base nos critérios definidos, registrar alterações, gerar alertas (manualmente ou automaticamente) e manter a rastreabilidade do desempenho do ativo.
Saída:
Dados atualizados de monitoramento. Registro de alertas ou desvios (automático ou manual). Subsídios para detecção de eventos, geração de alertas e tomada de decisão nas etapas do processo.

APÊNDICE E – ESPECIFICAÇÃO MGE AUTOMÁTICO (APENAS EXCEÇÃO)

5.1 Analisar Violação (Exceção)
Descrição:
Analisa e identifica as causas e impactos da exceção ou violação.
Atores Envolvidos:
- Analista TI. - Coordenador Técnico ou responsável pela análise de incidentes/problemas.
Etapas:
Se o processo estiver implantado: a) Avaliação formal detalhada (logs, histórico, métricas); b) Elaboração estruturada de relatório. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Avaliação empírica e informal baseada em registros mínimos (logs básicos, relatos verbais); b) Registro simplificado (planilha, e-mail ou relatório informal).
Recursos:
Se o processo estiver implantado: a) Sistema automatizado de monitoramento e análise. b) Templates formais de relatórios. Se o processo não estiver implantado (considera-se o mínimo necessário): a) Documentação manual (ex: planilha excel, e-mail, documento Word).
Entrada:
Alerta evento de exceção (alta criticidade).
Ação:
Gerar relatório detalhado do evento.
Saída:
Dados encaminhados para (5.2).
5.2 Definir Ação a ser Tomada
Descrição:
O incidente é classificado de acordo com a sua característica e, em seguida, são determinadas as ações a serem tomadas com base na sua gravidade e no impacto que ele tem na disponibilidade dos serviços.
Atores Envolvidos:
- Analista TI. - Coordenador Técnico ou responsável pela análise de incidentes/problemas.
Etapas:
Se o processo estiver implantado: a) Consultar Inventário e Base de Conhecimento formal; b) Elaborar plano formal de ação corretiva; c) Avaliar formalmente necessidade de autorização superior. Se o processo não estiver implantado (considera-se o mínimo desejável):

a) Avaliação informal com base em conhecimento técnico empírico; b) Registro simples das ações propostas; c) Decisão empírica sobre autorização superior.
Recursos:
Se o processo estiver implantado: a)Base de Conhecimento institucional. b) Inventário atualizado. c) Plano de Ação formal. Se o processo não estiver implantado (considera-se o mínimo necessário): a) Registro simples (planilha ou documento informal). b) Experiência empírica da equipe.
Entrada:
Inventário e Base de conhecimento.
Ação:
Definir ações corretivas necessárias.
Saída:
Decisão sobre necessidade de autorização superior: Caso sim: encaminha para etapa (5.3); Caso não: Encaminha para etapa (5.4).
5.3 Aguardar Autorização Superior
Descrição:
A ação a ser tomada é pausada até que a autorização (formal ou informar) do Superior seja concedida.
Atores Envolvidos:
- Gestor Superior ou Diretor de TI.
Etapas:
Se o processo estiver implantado: a) Solicitação formal documentada; b) Recebimento de autorização documentada. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Solicitação informal por telefone, e-mail ou reunião rápida; b) Registro mínimo da aprovação (e-mail ou verbalmente anotado).
Recursos:
Se o processo estiver implantado: a) Documentação formal (sistema de workflow ou e-mail institucional) Se o processo não estiver implantado (considera-se o mínimo necessário): a) Comunicação informal (telefone, WhatsApp, e-mail).
Entrada:
Decisão da etapa (5.2).
Ação:
Conceder autorização.
Saída:
Autorização obtida, encaminha para etapa (5.4).

5.4 Aguardar Autorização Superior
Descrição:
Executar medidas corretivas para resolver o incidente e restaurar os serviços.
Atores Envolvidos:
- Analista TI. - Coordenador Técnico ou responsável pela análise de incidentes/problemas.
Etapas:
Se o processo estiver implantado: a) Executar plano formal de ação registrado; b) Verificar formalmente restabelecimento da operação. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Execução direta com base no conhecimento da equipe; b) Avaliação empírica de retorno operacional.
Recursos:
Se o processo estiver implantado: a) Plano formal documentado (ferramenta ITSM ou documento estruturado). Se o processo não estiver implantado (considera-se o mínimo necessário): a) Registro simplificado (planilha, documento informal).
Entrada:
Plano de Ação, autorização (se aplicável).
Ação:
Executar ações corretivas definidas.
Saída:
Decisão sobre restabelecimento operacional do IC ou serviço: Caso sim: encaminha para etapa (5.6); Caso não: retorna para etapa (5.2).
5.5 Atualizar Base de Conhecimento
Descrição:
Atualiza as informações sobre as soluções adotadas para análise futura.
Atores Envolvidos:
- Analista TI. - Coordenador Técnico ou responsável pela análise de incidentes/problemas.
Etapas:
Se o processo estiver implantado: a) Registrar formalmente solução aplicada na Base de Conhecimento institucional. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Registro simples em documentos locais ou planilhas.
Recursos:
Se o processo estiver implantado: c) Base de conhecimento estruturada. Se o processo não estiver implantado (considera-se o mínimo desejável): d) Planilha ou documento local.
Entrada:

Ação executada com sucesso (1.20).
Ação:
Registrar solução adotada.
Saída:
Base atualizada e encaminha para a etapa (1.22).
5.6 Comunicar Partes Interessadas
Descrição:
Realiza comunicação clara e direta às partes interessadas sobre o incidente ou problema e sua resolução.
Atores Envolvidos:
- Analista TI. - Coordenador Técnico ou responsável pela análise de incidentes/problemas.
Etapas:
Se o processo estiver implantado: a) Comunicação formal e estruturada via e-mail institucional ou sistema ITSM. Se o processo não estiver implantado (considera-se o mínimo desejável): a) Comunicação informal por telefone, WhatsApp ou e-mail simples.
Recursos:
Se o processo estiver implantado: b) Ferramenta formal de comunicação institucional. Se o processo não estiver implantado (considera-se o mínimo desejável): b) Canais informais (telefone, e-mail simples, WhatsApp).
Entrada:
Solução registrada e Base atualizada (1.21).
Ação:
Comunicar resultado do tratamento.
Saída:
Avaliação final: Caso solucionado: encaminha para registro histórico (1.6); Caso contornado (sem solução definitiva): encaminha simultaneamente para: a) Gerenciamento de Problemas (1.14); b) Abertura formal de chamado (1.15).
5.7 Gerenciamento de Problema
Descrição:
Quando um evento é contornado, mas não possui uma solução definitiva, ele deve ser formalmente encaminhado para o processo de Gerenciamento de Problemas. Esse processo visa identificar a causa raiz da falha e propor ações corretivas estruturais.
Atores Envolvidos:
- Analista TI. - Coordenador Técnico ou responsável pela análise de incidentes/problemas.
Etapas:
Se o processo estiver implantado: a) Atender o chamado referente ao problema no sistema ITSM.

b) Iniciar a análise da causa raiz. c) Associar o problema a incidentes recorrentes (se houver). d) Propor ações corretivas definitivas. <u>Se o processo não estiver implantado (considera-se o mínimo desejável):</u> a) Registrar o problema de forma simplificada (planilha, e-mail ou documento informal). b) Designar responsável técnico. c) Conduzir análise ad hoc com base na experiência. d) Monitorar evolução do caso manualmente.
Recursos:
<u>Se o processo estiver implantado:</u> Módulo de Gerenciamento de Problemas do ITSM Base de Conhecimento Histórico técnico de incidentes <u>Se o processo não estiver implantado (considera-se o mínimo desejável):</u> a) Controle local (planilhas ou arquivos) b) Logs, registros manuais e conhecimento técnico.
Entrada:
Evento classificado como “contornado".
Ação:
Iniciar tratativa do problema em fluxo próprio.
Saída:
Evento tratado no fluxo de Gerenciamento de Problemas.

APÊNDICE F – DOCUMENTAÇÃO DOS ARTEFATOS

Este apêndice apresenta os modelos dos artefatos documentais destinados a orientar as equipes responsáveis pela implantação da prática da MGE. Cada *template* apresenta, de forma padronizada, a finalidade do documento, o escopo de aplicação, a estrutura mínima recomendada, as responsabilidades atribuídas e a periodicidade de atualização.

ARTEFATO DOCUMENTAL – PLANO DE AÇÃO

Versão: 1.0

Data: 25/06/2025

Artefato: Plano de Ação

Finalidade: Formalizar as ações a serem executadas diante de eventos de exceção, assegurando resposta coordenada, rastreável e eficaz para restaurar os serviços e mitigar impactos.

Estrutura sugerida:

- Identificação do Evento (ID, data/hora, descrição, origem);
- Classificação (urgência, impacto, criticidade);
- Descrição do Problema ou Falha;
- Objetivo da Ação;
- Ação a ser executada;
- Responsável pela execução;
- Recursos necessários;
- Prazo estimado de execução;
- Indicadores de verificação (se aplicável);
- Risco associado (se houver);
- Plano de comunicação (se necessário);
- Registro da execução e status.

Responsável pela Elaboração: Diretor / Gerente / Analista de Resposta a Incidentes.

Periodicidade de Atualização: Por ocorrência / conforme demanda.

ARTEFATO DOCUMENTAL – PLANO DE MELHORIAS

Versão: 1.0

Data: 25/06/2025

Artefato: Plano de Melhorias

Finalidade: Formalizar ações corretivas e preventivas com base nas análises dos eventos registrados, visando a melhoria contínua do processo.

Estrutura sugerida:

- Descrição da situação identificada;
- Causa raiz ou fator contribuidor;
- Ação de melhoria proposta (corretiva ou preventiva);
- Justificativa da ação;
- Responsável pela implementação;
- Prazo previsto;
- Indicadores de sucesso (KPIs);
- Status de acompanhamento.

Responsável pela Elaboração: Equipe técnica de TI ou responsável designado.

Periodicidade de Revisão: Trimestral / Conforme necessidade.

ARTEFATO DOCUMENTAL – PLANO DE MONITORAÇÃO

Versão: 1.0

Data: 25/06/2025

Artefato: Plano de Monitoração

Finalidade: Estabelecer os ativos, parâmetros, regras e responsabilidades do processo de monitoração.

Estrutura sugerida:

- Objetivo do plano;
- Serviços e ativos críticos a serem monitorados;
- Métricas e indicadores a serem coletados;
- Ferramentas e sistemas utilizados;
- *Thresholds* e regras de correlação de eventos;
- Responsabilidades e papéis envolvidos;
- Procedimentos de revisão e atualização do plano;
- Frequência de verificação dos parâmetros.

Responsável pela Elaboração: Equipe técnica de TI ou responsável designado.

Periodicidade de Revisão: Trimestral / Conforme necessidade.

ARTEFATO DOCUMENTAL – RELATÓRIO DE EVENTOS

Versão: 1.0

Data: 25/06/2025

Artefato: Relatório de Eventos

Finalidade: Consolidação e registro dos eventos monitorados no ambiente de TI para fins de análise, auditoria e melhoria contínua.

Estrutura sugerida:

- Identificador do Evento;
- Data e Hora;
- Tipo de Evento (Informativo, Alerta, Exceção);
- Sistema/Serviço de Origem;
- Classificação de Criticidade;
- Ação executada / Resposta aplicada;
- Responsável;
- Status final do evento;
- Observações.

Periodicidade de Emissão: Diário / Semanal / Sob demanda.

Responsável pela Emissão: Equipe técnica de TI, responsável designado pela monitoração.

APÊNDICE G – ESTRUTURA DE PAPÉIS E RESPONSABILIDADES (RACI) APLICADA AO FLUXO MGE

O presente apêndice reúne as matrizes RACI elaboradas para os diferentes fluxos que compõem o modelo institucional de MGE. Cada matriz documenta a distribuição de papéis e responsabilidades entre as equipes envolvidas, assegurando transparência, padronização operacional e aderência às boas práticas de governança de TI. A consolidação desses instrumentos permite à instituição compreender, implementar e auditar com precisão as responsabilidades atribuídas a cada etapa do processo, contribuindo para o fortalecimento da maturidade organizacional e para o alinhamento às diretrizes operacionais do modelo.

A legenda apresentada a seguir padroniza a interpretação das matrizes RACI, promovendo uniformidade na leitura dos papéis atribuídos às atividades dos diversos fluxos da MGE. Os códigos R (*Responsible*), A (*Accountable*), C (*Consulted*) e I (*Informed*) indicam, respectivamente, quem executa a tarefa, quem detém a responsabilidade final pelo resultado, quem oferece insumos técnicos ou validações e quem deve ser informado sobre o andamento ou desfecho da atividade. Essa padronização favorece a clareza organizacional, reforça a rastreabilidade das ações e contribui para a aplicação consistente das responsabilidades definidas em cada processo.

TABELA RACI – LEGENDA

Sigla	Descrição	Cor
R - *Responsible*	Responsável, executa a atividade	
A - *Accountable*	Autoridades aprovadores, tem responsabilidade final (entrega e resultados)	
C - *Consulted*	Profissionais consultados, fornece insumos técnicos ou validações	
I - *Informed*	Destinatários de Informação, comunicado do andamento ou resultado	

TABELA RACI – FLUXO MGE (1.0 A 1.22)

Etapa / Atividade	Diretor de TI	Equipe de Redes	Equipe de Banco de Dados	Equipe de Suporte
1.0 – Início / Start Automático	A	R	C	I
1.1 – Coletar Métricas, Logs e Status de Ativos	A	R	C	I
1.2 – Correlacionar Eventos e Identificar Padrões	A	R	C	I
1.3 – Evento Informativo (Registro Histórico)	A	R	I	I
1.4 – Evento de Alerta	A	R	C	I
1.5 – Evento de Exceção	A	R	C	I
1.6 – Registrar Evento (GLPI)	A	R	I	I
1.7 – Aplicar Matriz de Criticidade (Motor Fuzzy)	A	R	C	I
1.8 – Classificar e Direcionar Tratamento	A	R	C	I
1.9 – Prioridade Baixa (Avaliação e Registro)	A	R	C	I
1.10 – Prioridade Média (Encaminhamento)	A	R	C	R
1.11 – Prioridade Alta (Ação Imediata)	A	R	C	I
1.12 – Categorizar Evento	A	R	C	I
1.13 – Encaminhar p/ Gerenciamento de Incidentes	A	R	C	R
1.14 – Encaminhar p/ Gerenciamento de Problemas	A	R	C	R
1.15 – Abrir Chamado / Solicitação de Suporte	A	R	I	I
1.16 – Ação de Contorno	A	R	C	I
1.17 – Analisar Violação / Exceção	A	R	C	I
1.18 – Definir Ação a Ser Tomada	A	R	C	I
1.19 – Aguardar Autorização Superior	R	C	I	I

1.20 – Executar Ação (Operacional)	A	R	C	R
1.21 – Atualizar Base de Conhecimento	A	R	C	I
1.22 – Comunicar Partes Interessadas	A	R	C	R

TABELA RACI – FLUXO MGE MANUAL (2.0 A 2.5)

Etapa / Atividade	Diretor de TI	Equipe de Redes	Equipe de Banco de Dados	Equipe de Suporte
2.1 Escolher Item de Configuração (IC)	A	R	C	I
2.2 Coletar Dados	A	R	C	R
2.3 Analisar Dados	A	R	C	R
Decisão: Incidente ou Problema?	A	R	C	I
2.4 Encaminhar para Gerenciamento de Incidentes	A	R	C	R
2.5 Encaminhar para Gerenciamento de Problemas	A	R	C	R

TABELA RACI – PLANO DE MONITORAÇÃO (3.0 A 3.4)

Etapa / Atividade	Diretor de TI	Equipe de Redes	Equipe de Banco de Dados	Equipe de Suporte
3.1 Rever Processo de Monitoração	A	R	C	I
3.2 Analisar e Propor Melhorias	A	R	C	I
3.3 Validar Alterações	A	R	C	I
3.4 Atualizar Plano de Monitoração	A	R	C	I

TABELA RACI – MONITORAR (4.0)

Etapa / Atividade	Diretor de TI	Equipe de Redes	Equipe de Banco de Dados	Equipe de Suporte
4.1 Monitorar	A	R	C	I

TABELA RACI – FLUXO MGE APENAS EXCEÇÃO (5.0 A 5.7)

Etapa / Atividade	Diretor de TI	Equipe de Redes	Equipe de Banco de Dados	Equipe de Suporte
5.1 Analisar Violação (exceção)	A	R	C	R
5.2 Definir Ação a Ser Tomada	A	R	C	R
5.3 Aguardar Autorização Superior	A	R	I	I
5.4 Executar Ação (Operacional)	A	R	C	R
5.5 Atualizar Base de Conhecimento	A	R	C	R
5.6 Comunicar Partes Interessadas	A	R	I	R
5.7 Encaminhar para Gerenciamento de Problema	A	R	C	R

APÊNDICE H – QUESTIONÁRIO DE AVALIAÇÃO DE MATURIDADE

O presente questionário foi concebido para aferir o grau de maturidade institucional na prática de Monitoração e Gerenciamento de Eventos, em ambientes de Tecnologia da Informação, com fundamento nas recomendações da ITIL 4 e em referenciais complementares de governança. Seu propósito é evidenciar capacidades e lacunas que impactam a detecção, a correlação e a resposta a eventos, permitindo que organizações públicas ou privadas, independentemente de já adotarem formalmente tais *frameworks*, desenvolvam planos de evolução contínua da prática e, por conseguinte, da confiabilidade dos serviços de TIC.

O QDA contempla oito eixos analíticos: *Processos e Procedimentos; Resposta a Eventos e Melhoria Contínua; Tecnologia e Ferramentas; Governança e Estratégia; Cultura Organizacional; Pessoas e Capacitação; Gestão da Informação e Dados; Escalabilidade e Crescimento*, de modo que cada questão possa contribuir para um ou mais desses vetores de avaliação. Essa abordagem multifacetada garante visão holística sobre fatores operacionais, humanos e estratégicos que sustentam a MGE.

As 25 questões utilizam uma escala de 05 pontos mapeada a fatores multiplicativos (FM): Concordo Totalmente (3), Concordo (1), Neutro (0), Discordo (-1) e Discordo Totalmente (-3). Essa parametrização converte percepções qualitativas em valores quantitativos, permitindo o cálculo objetivo dos impactos de cada resposta sobre os eixos avaliados. Os pesos atribuídos a cada questão, mantidos ocultos aos respondentes para evitar vieses, refletem a relevância relativa de cada dimensão na prática de MGE e foram definidos com base em literatura especializada e experiência profissional.

Para cada eixo, soma-se o produto (FM x Peso) das questões associadas, resultando em um indicador que posiciona a organização em um continuum de maturidade. Esses valores orientam a priorização de intervenções, a definição de metas de curto e médio prazo e a monitoração de progressos ao longo do tempo. Assim, o questionário transcende a simples coleta de opiniões, funcionando como instrumento de gestão do conhecimento e de suporte à tomada de decisão baseada em evidências.

Todas as perguntas do QDA devem ser respondidas utilizando a escala padronizada abaixo, que assegura uniformidade na mensuração da maturidade e simplifica a tabulação dos resultados:

Alternativa	Peso
a) Concordo Totalmente: A prática está plenamente implementada e é eficaz.	+3
b) Concordo: A prática está implementada, mas pode melhorar.	+1
c) Neutro: Não há clareza ou há implementação parcial.	0
d) Discordo: A prática existe de forma insatisfatória.	-1
e) Discordo Totalmente: A prática não existe ou é inexistente na rotina.	-3

Nas páginas seguintes, cada questão do QDA é listada, acompanhada da tabela que associa seus pesos aos respectivos eixos.

Questão 1	
1. A organização utiliza algum meio ou ferramenta para realizar a monitoração e o gerenciamento de eventos de TI, ainda que de forma parcial ou não formalizada?	
Eixo	**Peso**
Escalabilidade e Crescimento	0
Pessoas e Capacitação	0
Governança e Estratégia	3
Processos e Procedimentos	1
Gestão da Informação e Dados	0
Cultura Organizacional	1
Tecnologia e Ferramentas	0
Resposta a Eventos e Melhoria Contínua	0
Questão 2	
2. A organização utiliza uma ferramenta centralizada para monitorar, em tempo real, seus sistemas, serviços e infraestrutura de TI?	
Eixo	**Peso**
Escalabilidade e Crescimento	0
Pessoas e Capacitação	0
Governança e Estratégia	0
Processos e Procedimentos	1
Gestão da Informação e Dados	1

Cultura Organizacional	0
Tecnologia e Ferramentas	3
Resposta a Eventos e Melhoria Contínua	1
Questão 3	
3. Os eventos de TI são classificados com base em criticidade e impacto para o negócio?	
Eixo	**Peso**
Escalabilidade e Crescimento	0
Pessoas e Capacitação	0
Governança e Estratégia	1
Processos e Procedimentos	3
Gestão da Informação e Dados	1
Cultura Organizacional	0
Tecnologia e Ferramentas	1
Resposta a Eventos e Melhoria Contínua	1
Questão 4	
4. A monitoração contempla tanto a detecção de falhas quanto a previsão de problemas?	
Eixo	**Peso**
Escalabilidade e Crescimento	2
Pessoas e Capacitação	0
Governança e Estratégia	0
Processos e Procedimentos	2
Gestão da Informação e Dados	2
Cultura Organizacional	0
Tecnologia e Ferramentas	3
Resposta a Eventos e Melhoria Contínua	2
Questão 5	
5. A quantidade e a qualidade dos alertas emitidos pela ferramenta de monitoração são adequadas e evitam ruídos ou alarmes desnecessários?	
Eixo	**Peso**
Escalabilidade e Crescimento	1
Pessoas e Capacitação	0

Governança e Estratégia	0
Processos e Procedimentos	2
Gestão da Informação e Dados	1
Cultura Organizacional	0
Tecnologia e Ferramentas	3
Resposta a Eventos e Melhoria Contínua	1
Questão 6	
6. Os eventos são automaticamente correlacionados para facilitar a identificação da causa raiz?	
Eixo	**Peso**
Escalabilidade e Crescimento	1
Pessoas e Capacitação	0
Governança e Estratégia	0
Processos e Procedimentos	2
Gestão da Informação e Dados	2
Cultura Organizacional	0
Tecnologia e Ferramentas	3
Resposta a Eventos e Melhoria Contínua	1
Questão 7	
7. A equipe de TI compreende claramente o processo de gerenciamento de eventos?	
Eixo	**Peso**
Escalabilidade e Crescimento	0
Pessoas e Capacitação	3
Governança e Estratégia	0
Processos e Procedimentos	2
Gestão da Informação e Dados	0
Cultura Organizacional	1
Tecnologia e Ferramentas	0
Resposta a Eventos e Melhoria Contínua	1
Questão 8	
8. Existe um responsável ou equipe dedicada à monitoração de eventos?	
Eixo	**Peso**
Escalabilidade e Crescimento	1

Pessoas e Capacitação	2
Governança e Estratégia	1
Processos e Procedimentos	2
Gestão da Informação e Dados	0
Cultura Organizacional	1
Tecnologia e Ferramentas	0
Resposta a Eventos e Melhoria Contínua	1
Questão 9	
9. A monitoração abrange todos os serviços críticos da organização?	
Eixo	**Peso**
Escalabilidade e Crescimento	1
Pessoas e Capacitação	0
Governança e Estratégia	2
Processos e Procedimentos	2
Gestão da Informação e Dados	1
Cultura Organizacional	1
Tecnologia e Ferramentas	2
Resposta a Eventos e Melhoria Contínua	2
Questão 10	
10. A TI é capaz de agir proativamente a partir dos eventos monitorados?	
Eixo	**Peso**
Escalabilidade e Crescimento	2
Pessoas e Capacitação	2
Governança e Estratégia	1
Processos e Procedimentos	2
Gestão da Informação e Dados	1
Cultura Organizacional	1
Tecnologia e Ferramentas	2
Resposta a Eventos e Melhoria Contínua	3
Questão 11	
11. Há integração entre a ferramenta de monitoração e o sistema de chamados (Service Desk)?	
Eixo	**Peso**

Escalabilidade e Crescimento	1
Pessoas e Capacitação	1
Governança e Estratégia	1
Processos e Procedimentos	1
Gestão da Informação e Dados	1
Cultura Organizacional	1
Tecnologia e Ferramentas	1
Resposta a Eventos e Melhoria Contínua	1
Questão 12	
12. Os eventos são registrados, analisados e utilizados para fins de melhoria contínua?	
Eixo	**Peso**
Escalabilidade e Crescimento	1
Pessoas e Capacitação	1
Governança e Estratégia	1
Processos e Procedimentos	2
Gestão da Informação e Dados	2
Cultura Organizacional	1
Tecnologia e Ferramentas	0
Resposta a Eventos e Melhoria Contínua	3
Questão 13	
13. Indicadores e métricas de eventos são periodicamente analisados pela gestão de TI?	
Eixo	**Peso**
Escalabilidade e Crescimento	1
Pessoas e Capacitação	0
Governança e Estratégia	2
Processos e Procedimentos	2
Gestão da Informação e Dados	3
Cultura Organizacional	1
Tecnologia e Ferramentas	0
Resposta a Eventos e Melhoria Contínua	2
Questão 14	
14. A gestão da TI utiliza dados de eventos para tomar decisões estratégicas?	

Eixo	Peso
Escalabilidade e Crescimento	2
Pessoas e Capacitação	0
Governança e Estratégia	3
Processos e Procedimentos	1
Gestão da Informação e Dados	3
Cultura Organizacional	1
Tecnologia e Ferramentas	0
Resposta a Eventos e Melhoria Contínua	1
Questão 15	
15. A monitoração dos serviços de TI é realizada de forma contínua (24/7) e segue critérios definidos de acordo com a criticidade de cada serviço?	
Eixo	**Peso**
Escalabilidade e Crescimento	0
Pessoas e Capacitação	0
Governança e Estratégia	2
Processos e Procedimentos	2
Gestão da Informação e Dados	0
Cultura Organizacional	0
Tecnologia e Ferramentas	2
Resposta a Eventos e Melhoria Contínua	3
Questão 16	
16. Existe documentação atualizada dos processos e procedimentos de monitoração?	
Eixo	**Peso**
Escalabilidade e Crescimento	1
Pessoas e Capacitação	1
Governança e Estratégia	1
Processos e Procedimentos	3
Gestão da Informação e Dados	2
Cultura Organizacional	1
Tecnologia e Ferramentas	0
Resposta a Eventos e Melhoria Contínua	2
Questão 17	

17. Novas implementações de sistemas já consideram requisitos de monitoração desde o início?	
Eixo	**Peso**
Escalabilidade e Crescimento	3
Pessoas e Capacitação	0
Governança e Estratégia	2
Processos e Procedimentos	2
Gestão da Informação e Dados	2
Cultura Organizacional	1
Tecnologia e Ferramentas	2
Resposta a Eventos e Melhoria Contínua	2
Questão 18	
18. A monitoração contempla também segurança da informação (eventos suspeitos, acessos não autorizados)?	
Eixo	**Peso**
Escalabilidade e Crescimento	2
Pessoas e Capacitação	0
Governança e Estratégia	2
Processos e Procedimentos	2
Gestão da Informação e Dados	3
Cultura Organizacional	1
Tecnologia e Ferramentas	2
Resposta a Eventos e Melhoria Contínua	2
Questão 19	
19. O ciclo de vida do evento (detecção, registro, resposta, encerramento) é formalizado?	
Eixo	**Peso**
Escalabilidade e Crescimento	2
Pessoas e Capacitação	1
Governança e Estratégia	1
Processos e Procedimentos	3
Gestão da Informação e Dados	2
Cultura Organizacional	0

Tecnologia e Ferramentas	1
Resposta a Eventos e Melhoria Contínua	3
Questão 20	
20. A alta administração compreende o valor da prática de monitoração de eventos para o negócio?	
Eixo	**Peso**
Escalabilidade e Crescimento	1
Pessoas e Capacitação	1
Governança e Estratégia	3
Processos e Procedimentos	1
Gestão da Informação e Dados	0
Cultura Organizacional	2
Tecnologia e Ferramentas	0
Resposta a Eventos e Melhoria Contínua	1
Questão 21	
21. Os usuários percebem melhora na disponibilidade dos serviços devido à prática de monitoração?	
Eixo	**Peso**
Escalabilidade e Crescimento	1
Pessoas e Capacitação	1
Governança e Estratégia	1
Processos e Procedimentos	2
Gestão da Informação e Dados	0
Cultura Organizacional	2
Tecnologia e Ferramentas	1
Resposta a Eventos e Melhoria Contínua	3
Questão 22	
22. A organização realiza capacitação contínua sobre boas práticas de monitoração e gerenciamento de eventos, como por exemplo as propostas pela ITIL?	
Eixo	**Peso**
Escalabilidade e Crescimento	1
Pessoas e Capacitação	3
Governança e Estratégia	1

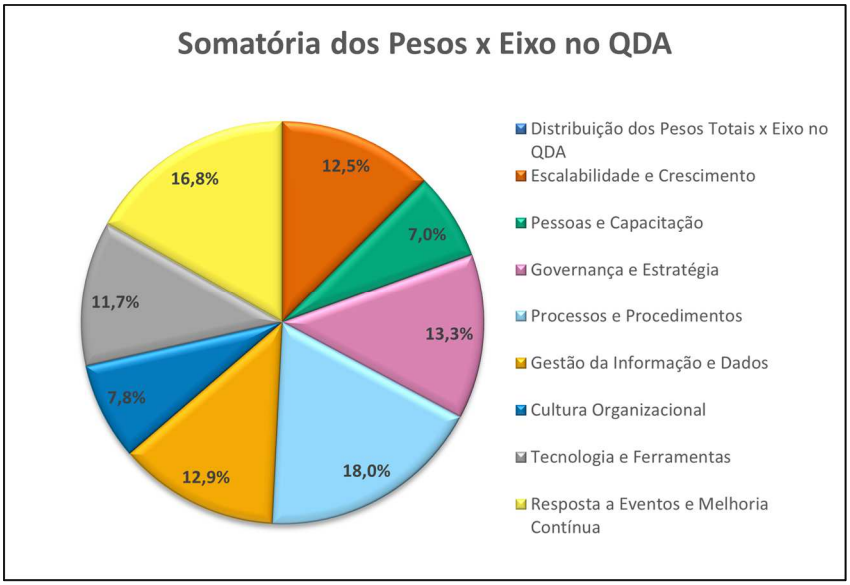
Processos e Procedimentos	1
Gestão da Informação e Dados	1
Cultura Organizacional	2
Tecnologia e Ferramentas	0
Resposta a Eventos e Melhoria Contínua	2
Questão 23	
23. Há revisões periódicas da maturidade da prática de eventos e planos de ação definidos?	
Eixo	**Peso**
Escalabilidade e Crescimento	2
Pessoas e Capacitação	1
Governança e Estratégia	2
Processos e Procedimentos	3
Gestão da Informação e Dados	1
Cultura Organizacional	1
Tecnologia e Ferramentas	0
Resposta a Eventos e Melhoria Contínua	3
Questão 24	
24. A organização está preparada para evoluir a monitoração com uso de inteligência artificial ou *analytics*?	
Eixo	**Peso**
Escalabilidade e Crescimento	3
Pessoas e Capacitação	1
Governança e Estratégia	1
Processos e Procedimentos	1
Gestão da Informação e Dados	2
Cultura Organizacional	1
Tecnologia e Ferramentas	3
Resposta a Eventos e Melhoria Contínua	1
Questão 25	
25. A organização está preparada para expandir e adaptar suas práticas de monitoração e gerenciamento de eventos conforme o crescimento da infraestrutura de TI, sem comprometer a eficiência?	

Eixo	Peso
Escalabilidade e Crescimento	3
Pessoas e Capacitação	0
Governança e Estratégia	3
Processos e Procedimentos	1
Gestão da Informação e Dados	2
Cultura Organizacional	0
Tecnologia e Ferramentas	1
Resposta a Eventos e Melhoria Contínua	1

A seguir, apresenta-se a análise quantitativa dos pesos atribuídos a cada eixo de maturidade ao longo das 25 questões QDA. Para cada eixo, somaram-se os valores dos pesos que lhe foram designados em cada pergunta, resultando em um indicador agregado da presença e relevância de cada dimensão na avaliação da maturidade da prática de Monitoramento e Gerenciamento de Eventos.

Esse procedimento permite aferir, de modo transparente e fundamentado, se o instrumento contempla de maneira equilibrada os diferentes domínios avaliativos ou se há concentração de ênfase em determinados aspectos do modelo.

O gráfico a seguir sintetiza a distribuição percentual dos pesos totais por eixo, facilitando a visualização comparativa da cobertura de cada dimensão dentro do instrumento. Assim, é possível identificar rapidamente quais eixos tiveram maior representatividade e assegurar a coerência metodológica na estruturação do questionário, reforçando sua validade como ferramenta diagnóstica de maturidade institucional em MGE.



Distribuição percentual dos pesos totais atribuídos a cada eixo de maturidade no QDA da prática de MGE. Fonte: Autor.

Multiplicação pelo Peso do Eixo

Para cada questão, cada eixo possui um peso predefinido (P). O impacto da resposta em cada eixo é obtido multiplicando o fator de resposta (FM) pelo peso do eixo naquela pergunta.

TRABALHOS PUBLICADOS PELO AUTOR

Trabalhos publicados pelo autor durante o programa:

1. GARANHANI JUNIOR, L. C.; BARROS, Rodolfo Miranda de; BARROS, Vanessa Tavares de Oliveira. “A model for implementing the ITIL 4 event management and monitoring practice in a public organization”. In: 20th CONTECSI – *International Conference on Information Systems and Technology Management* (Virtual). – February 5-7, 2024, TECSI-FEA USP, São Paulo / Brasil. ISSN 2448-1041. DOI: 10.5748/20CONTECSI/PSE/ITM/7283.
2. GARANHANI JUNIOR, L. C. et al. Structured event monitoring and management model with ITIL 4: Application and maturity diagnosis in a municipal public agency. *Procedia Computer Science*, v. 278, p. 450–457, 2026. DOI: 10.1016/j.procs.2026.03.012.

Trabalhos aceitos e ainda não publicados durante o programa:

3. GARANHANI JUNIOR, L. C. et al. IT Event Management in the Municipal Public Sector: An Automated Architecture Based on ITIL 4 and Fuzzy Inference. Trabalho aceito para apresentação/publicação no XXII Simpósio Brasileiro de Sistemas de Informação (SBSI 2026), Vitória, ES, Brasil, 25-28 maio 2026. No prelo.
4. GARANHANI JUNIOR, L. C. et al. Uma Arquitetura para Gerenciamento Automatizado de Eventos de TI em Governos Municipais: Integrando ITIL 4, Zabbix, um Mecanismo de Inferência Fuzzy e GLPI. In: CISTI’2026 – *21st Iberian Conference on Information Systems and Technologies*, University of Santiago de Compostela, Santiago de Compostela, Espanha, 17-20 jun. 2026. No prelo.