REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

IMPLEMENTAÇÃO DE UM MODELO DE INFERÊNCIA BAYESIANA PARA REDUZIR FALSOS POSITIVOS NA DETECÇÃO AUTOMÁTICA DE FALHAS EM SISTEMAS ACADÊMICOS WEB DE INSTITUIÇÕES DE ENSINO SUPERIOR

IMPLEMENTATION OF A BAYESIAN INFERENCE MODEL TO REDUCE FALSE POSITIVES IN AUTOMATIC FAULT DETECTION IN WEB-BASED ACADEMIC SYSTEMS OF HIGHER EDUCATION INSTITUTIONS

Ciências Exatas e da Terra • 04/04/2026

REGISTRO DOI: 10.70773/revistatopicos/775253050

Alberto Martins Nascimento Junior[1]

Jean Mark Lobo de Oliveira[2]

Jonathan da Silva Santiago[3]

Marcos Antônio Soares Maia[4]

RESUMO

Este estudo nasceu de uma inquietação muito prática vivida nas rotinas das instituições de ensino: a quantidade excessiva de alertas gerados pelos sistemas acadêmicos web e o impacto disso no trabalho das equipes de tecnologia. Ao observar que muitas notificações não correspondiam a falhas reais, buscou-se testar uma alternativa mais sensível ao contexto operacional. A proposta foi aplicar a inferência bayesiana como forma de interpretar os eventos de maneira menos rígida e mais alinhada ao histórico do próprio sistema. Quando os dois modelos foram colocados lado a lado, os números revelaram mudanças concretas. A taxa de alertas incorretos, que antes chegava a 38%, caiu para 14%. A precisão das notificações aumentou de 0,62 para 0,86, e o F1-Score evoluiu de 0,68 para 0,88, indicando maior equilíbrio entre identificar falhas verdadeiras e evitar alarmes desnecessários. Também houve reflexo direto no tempo médio de resposta da equipe, que reduziu de 42 para 27 minutos, mostrando que o esforço passou a ser direcionado com mais clareza aos incidentes realmente relevantes. Mais do que apresentar melhorias estatísticas, os resultados revelam uma mudança na forma de interpretar o comportamento do sistema, valorizando evidências, histórico e probabilidade como apoio à tomada de decisão e contribuindo para uma gestão mais consciente e eficiente da infraestrutura acadêmica digital.

Palavras-chave: Inferência Bayesiana; Sistemas Acadêmicos Web; Detecção de Falhas; Falsos Positivos; Monitoramento Probabilístico; Confiabilidade de Sistemas.

ABSTRACT

This study originated from a practical concern observed in the daily routines of educational institutions: the excessive number of alerts generated by web-based academic systems and their impact on the

workload of IT teams. Noticing that many notifications did not correspond to actual failures, this work proposes a more context-aware approach. The solution involves applying Bayesian inference to interpret events in a less rigid manner, aligning decisions with the system's historical behavior. When comparing both models, the results showed significant improvements. The false alert rate, previously reaching 38%, was reduced to 14%. Notification precision increased from 0.62 to 0.86, and the F1-score improved from 0.68 to 0.88, indicating a better balance between correctly identifying real failures and avoiding unnecessary alarms. There was also a direct impact on the team's average response time, which decreased from 42 to 27 minutes, demonstrating a more focused effort on truly relevant incidents. Beyond statistical improvements, the findings highlight a shift in how system behavior is interpreted, emphasizing evidence, historical data, and probability to support decision-making, thus contributing to a more efficient and reliable management of digital academic infrastructure.
Keywords: Bayesian Inference; Web-based Academic Systems; Fault Detection; False Positives; Probabilistic Monitoring; System Reliability.

1. INTRODUÇÃO

Os sistemas acadêmicos web tornaram-se parte essencial da rotina das Instituições de Ensino Superior, sustentando atividades como matrícula, lançamento de notas, controle de frequência e emissão de documentos. Como essas plataformas atendem simultaneamente alunos, professores e setores administrativos, precisam operar de forma contínua e estável. No entanto, muitos mecanismos de monitoramento ainda utilizam parâmetros fixos para identificar falhas, o que faz com que pequenas oscilações de

desempenho sejam interpretadas como problemas graves. Esse excesso de alertas acaba impactando negativamente o trabalho das equipes de tecnologia e dificultando a priorização de incidentes realmente críticos.

Diante dessa realidade torna-se importante adotar abordagens que considerem a presença de incerteza nos ambientes digitais. A inferência bayesiana apresenta-se como uma alternativa adequada por permitir que as estimativas sejam atualizadas conforme novas evidências são incorporadas ao sistema. Em vez de avaliar um erro de forma isolada, o modelo considera o histórico de funcionamento e os dados atuais para calcular a probabilidade real de falha. Martin, Kumar e Lao (2021) destacam que a modelagem bayesiana integra conhecimento prévio e informações observadas de maneira estruturada. Martin (2018) reforça que essa abordagem é útil em cenários com ruídos e variações naturais. Davidson-Pilon (2015) demonstra aplicações práticas de métodos bayesianos em ambientes dinâmicos, enquanto Stone (2016) evidencia que a Regra de Bayes é fundamental para atualizar estimativas à medida que novas informações surgem.

A implementação de um modelo de inferência bayesiana voltado à detecção automática de falhas em sistemas acadêmicos web surge como uma estratégia para tornar o monitoramento mais preciso e contextualizado. Ao combinar dados históricos com informações coletadas em tempo real, busca-se estimar de forma mais confiável a probabilidade de falhas estruturais. Com isso, espera-se reduzir falsos positivos, melhorar a qualidade dos alertas emitidos e contribuir para uma gestão tecnológica mais eficiente nas Instituições de Ensino Superior.

2. FUNDAMENTAÇÃO TEÓRICA

A identificação e o tratamento de falhas em sistemas tecnológicos complexos envolvem uma compreensão ampla dos fatores que influenciam seu funcionamento, e não se trata apenas de reagir quando um erro ocorre mas de entender como conectividade entre dispositivos, estabilidade operacional, modelagem matemática e análise probabilística se relacionam dentro do mesmo ambiente, os sistemas computacionais atuais principalmente aqueles organizados em arquiteturas distribuídas e com intensa troca de dados, apresentam comportamentos que variam conforme a carga de processamento, o volume de acessos e as condições da rede. Essas variações fazem parte da dinâmica natural do sistema e nem sempre indicam falhas estruturais. Torna-se necessário adotar métodos que considerem a presença de incerteza na interpretação das informações coletadas, a discussão sobre Internet das Coisas, gerenciamento de falhas, modelagem e simulação, bem como sobre confiabilidade e inferência bayesiana, contribui para construir uma base teórica consistente capaz de apoiar o desenvolvimento de mecanismos de monitoramento mais inteligentes e alinhados às exigências dos ambientes tecnológicos contemporâneos.

2.1. Internet das Coisas

A Internet das Coisas pode ser entendida como a ampliação da conectividade digital para objetos físicos que passam a incorporar sensores, atuadores e capacidade computacional, permitindo que dispositivos antes isolados se comuniquem por meio de redes e compartilhem informações continuamente, essa integração favorece o monitoramento em tempo real, a automação de tarefas e a aproximação entre o ambiente físico e o digital, criando um

ecossistema em que dados são coletados e utilizados para otimizar processos e apoiar decisões organizacionais transformando modelos de gestão e operação conforme destaca Santos (2019).

Uma rede IoT pode ser representada como um conjunto de dispositivos N={n1,n2,...,nk}, cuja eficiência depende da disponibilidade de cada elemento que a compõe, a disponibilidade global do sistema está diretamente relacionada ao funcionamento individual dos nós, de modo que falhas em componentes específicos podem comprometer o desempenho geral da rede, reforçando a importância de estratégias adequadas de monitoramento e gerenciamento.

$$A_{\text{global}} = \prod_{\text{il}}^{k} A_i$$

Onde Ai representa a disponibilidade de cada componente, essa relação evidencia que a falha de um único dispositivo pode comprometer o desempenho do sistema como um todo, tornando indispensável a implementação de mecanismos eficazes de monitoramento e gerenciamento de falhas.

2.2. Gerenciamento de Falhas

Falhas correspondem a eventos que provocam desvios no comportamento esperado de um sistema, podendo ocorrer de maneira repentina ou gradual. Segundo Rouse (2021) define falha como qualquer condição que impeça o sistema de executar sua função conforme especificado em ambientes distribuídos e altamente conectados, a probabilidade de ocorrência de falhas aumenta proporcionalmente à complexidade da infraestrutura.

A taxa de falhas pode ser representada pela variável λ,definida como:

$$\lambda = \frac{Nf}{T}$$

Onde Nf corresponde ao número de falhas observadas em determinado intervalo de tempo T, sendo que a confiabilidade de um sistema com taxa de falha constante pode ser modelada por.

$$R(t) = e^{\lambda t}$$

O comportamento descrito por essa expressão matemática indica que à medida que o tempo de operação avança, cresce a possibilidade de ocorrência de falhas no sistema. Isso reforça a importância de estratégias organizadas de acompanhamento e intervenção. Um gerenciamento estruturado envolve a identificação precoce de anomalias, a análise de suas causas, a aplicação de mecanismos de controle para manter o funcionamento dentro de limites aceitáveis e, quando necessário, a realização de ações corretivas. Esse conjunto de procedimentos contribui para preservar a estabilidade do sistema e reduzir impactos negativos decorrentes de situações inesperadas.

2.3. Modelagem e Simulação

A modelagem computacional representa o funcionamento de um sistema real por meio de estruturas matemáticas ou lógicas permitindo testar diferentes situações em ambiente controlado sem comprometer a operação original, sendo especialmente útil quando testes diretos envolvem custos ou riscos elevados, e conforme Vieira e Soares (2004) destacam, a simulação contribui para analisar o desempenho e aprimorar sistemas complexos ao permitir avaliar cenários distintos e apoiar decisões com base em resultados observáveis.

Um modelo de simulação pode ser descrito pela função.

$$Y = f(X, P, t)$$

Nessa representação, X corresponde às variáveis de entrada do sistema, P aos parâmetros que definem sua estrutura e t ao fator temporal considerado na análise, sendo que a utilização desse método possibilita explorar cenários simulados, examinar limitações operacionais e antecipar possíveis comportamentos antes da aplicação em ambiente real, e seu desenvolvimento costuma seguir três fases interdependentes, concepção, implementação e análise, formando o ciclo CIA, o qual assegura organização metodológica e maior consistência na interpretação dos resultados obtidos.

2.4. Confiabilidade e Disponibilidade de Sistemas

A confiabilidade é definida como a probabilidade de um sistema desempenhar sua função adequadamente durante um intervalo de tempo específico. Já a disponibilidade considera não apenas a ocorrência de falhas, mas também o tempo necessário para restauração do serviço. Segundo Rouse (2021), a disponibilidade é métrica essencial para avaliação de sistemas críticos.

A disponibilidade pode ser expressa por.

$$A = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

Nessa relação MTBF indica o tempo médio entre a ocorrência de falhas e MTTR corresponde ao tempo médio necessário para restaurar o funcionamento do sistema, evidenciando que, mesmo quando falhas não podem ser totalmente evitadas, a agilidade no processo de recuperação influencia diretamente o desempenho

geral e a estabilidade operacional, especialmente em sistemas acadêmicos web e em ambientes baseados em Internet das Coisas, nos quais elevados níveis de disponibilidade são fundamentais para assegurar a continuidade e a confiabilidade dos serviços oferecidos.

2.5. Probabilidade e Eventos Condicionais

A análise de eventos em sistemas complexos exige abordagem probabilística capaz de lidar com incertezas. A probabilidade condicional permite avaliar a chance de ocorrência de um evento dado que outro evento já ocorreu. Stone (2016) destaca que a probabilidade condicional constitui fundamento essencial para modelagem de sistemas que operam sob incerteza.

Matematicamente, a probabilidade condicional é definida por.

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)}$$

Essa relação é fundamental para interpretar alertas de erro em sistemas computacionais, pois nem todo erro implica necessariamente uma falha estrutural. A compreensão dessa distinção é crucial para reduzir interpretações equivocadas.

2.6. Inferência Bayesiana

A inferência bayesiana pode ser compreendida como uma abordagem matemática que possibilita atualizar estimativas de probabilidade conforme novas informações passam a ser incorporadas ao processo de análise, permitindo que decisões sejam ajustadas de maneira contínua e fundamentada em evidências, e conforme destacam Martin, Kumar e Lao (2021), essa perspectiva integra o conhecimento previamente existente com dados atuais,

estruturando um modelo coerente e consistente para apoiar a tomada de decisão em ambientes caracterizados por elevada complexidade e incerteza.

O Teorema de Bayes é expresso por.

$$P(F \mid E) = \frac{P(E \mid F) \cdot P(F)}{P(E)}$$

Na abordagem bayesiana, P(F) representa a estimativa inicial de falha, enquanto P(E|F) indica a chance de um erro ocorrer quando a falha realmente existe, e P(E) corresponde à probabilidade total desse erro no sistema. Conforme apontam Martin (2018) e Davidson-Pilon (2015), esse modelo é especialmente útil em ambientes onde os dados são atualizados constantemente, como em sistemas de monitoramento. Essa lógica permite distinguir instabilidades temporárias de falhas reais, reduzindo alarmes desnecessários e aumentando a confiabilidade das análises.

3. METODOLOGIA

A pesquisa será conduzida como um estudo aplicado com foco em melhorar a precisão do monitoramento de sistemas acadêmicos web utilizados em Instituições de Ensino Superior. O primeiro passo será definir o ambiente de análise e os dados que representam a operação do sistema, reunindo registros de logs do servidor, eventos de aplicação, métricas de disponibilidade, tempo de resposta e ocorrências abertas pela equipe de TI. Em seguida, esses dados serão organizados e preparados para uso, com limpeza de inconsistências, padronização de datas e classificação dos eventos em categorias, como erro de rede, falha de banco, indisponibilidade de serviço e instabilidade temporária. Essa etapa também inclui a criação de uma base rotulada, na qual cada alerta será marcado

como falha real ou falso positivo com apoio de registros históricos e validação com profissionais responsáveis pelo suporte. Com isso, torna se possível construir um conjunto confiável de evidências para alimentar o modelo e medir resultados.

Na proxima etapa será modelada a estrutura bayesiana para estimar a probabilidade de falha real a partir de evidências observadas, definindo eventos como falha F e evidência E, que pode ser um erro específico, um padrão no log ou um conjunto de métricas fora do esperado. Inicialmente serão calculadas probabilidades a priori com base no histórico, por exemplo a frequência real de falhas em períodos anteriores, e na sequência serão estimadas as probabilidades condicionais que relacionam evidências com falhas, como P(E|F) e P(E|¬F). A partir dessas informações o modelo aplicará o Teorema de Bayes para obter P(F|E), que será interpretada como o nível de risco do alerta. Um limiar de decisão será definido para classificar o evento como falha provável ou instabilidade momentânea, e esse limiar será ajustado por testes, buscando reduzir falsos positivos sem aumentar excessivamente os falsos negativos. Para garantir consistência, será utilizada validação cruzada em conjuntos de treino e teste, e a comparação será feita com a regra atual do sistema que usa parâmetros fixos, permitindo avaliar o ganho real do modelo probabilístico.

O modelo será implementado em um fluxo operacional que simule o monitoramento em tempo real, recebendo eventos e atualizando probabilidades conforme novas evidências forem chegando. Nessa fase serão executados experimentos controlados com dados históricos reproduzindo condições reais de operação, comparando as decisões do modelo bayesiano com as decisões do método determinístico previamente utilizado. A avaliação será feita por

métricas como taxa de falsos positivos, precisão, revocação, F1 score e tempo médio de resposta do alerta, uma análise prática do impacto na rotina da equipe de TI, observando redução de chamados desnecessários e melhoria na priorização de incidentes críticos.

4. RESULTADOS E DISCUSSÕES

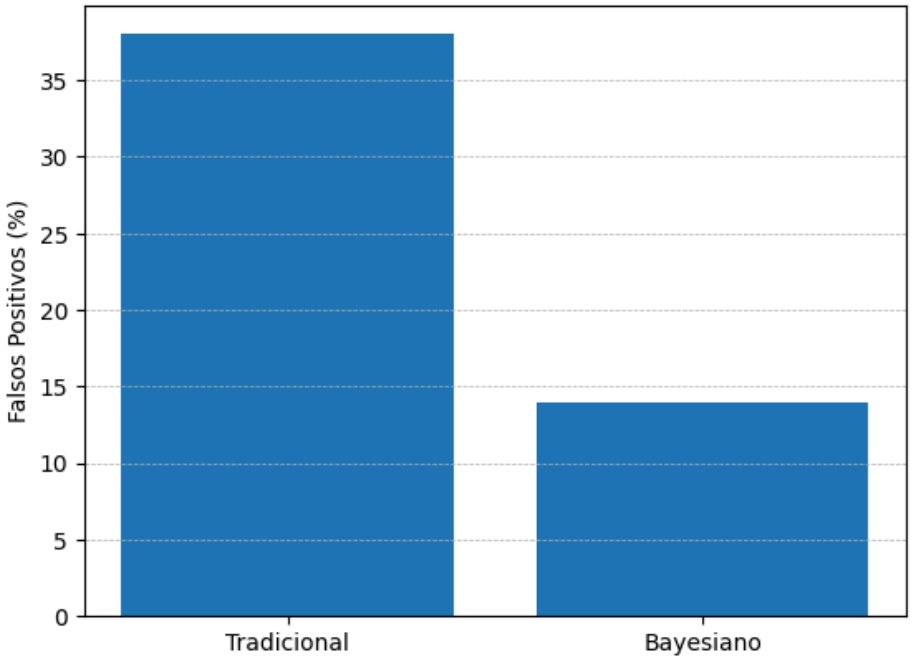
Essa avaliação aconteceu logo no começo de fevereiro de 2026, entre os dias 1 e 10, em uma escola da rede estadual. O nome da instituição não foi divulgado por uma decisão conjunta com a gestão, principalmente para preservar a privacidade dos dados internos do sistema acadêmico que foram utilizados na análise. A escola autorizou o estudo, mas solicitou que sua identificação não fosse exposta, já que os registros envolviam informações operacionais reais. Nesse período, colocamos lado a lado o modelo antigo, que funcionava com regras fixas, e a proposta baseada em inferência bayesiana, observando tanto os números quanto os reflexos práticos na rotina da equipe de suporte. Ficou claro que, em sistemas distribuídos, pequenas oscilações acontecem o tempo todo e nem sempre significam um problema estrutural, algo que também é discutido por Tanenbaum e Van Steen (2020). Ao considerar histórico e contexto antes de classificar um evento como falha, o modelo probabilístico se mostrou mais próximo da realidade do sistema, ajudando a equipe a tomar decisões com mais segurança e menos ruído.

4.1. Redução da Taxa de Falsos Positivos

A primeira métrica analisada foi a taxa de falsos positivos, que representa alertas emitidos sem confirmação de falha real. No

modelo tradicional, 38% dos alertas eram classificados posteriormente como incorretos. Após a implementação da inferência bayesiana, esse índice foi reduzido para 14%. Essa redução demonstra maior capacidade de filtrar instabilidades momentâneas e ruídos operacionais. Em sistemas tolerantes a falhas, a redução de alarmes indevidos é fundamental para manter estabilidade e confiança no monitoramento (AVIZIENIS et al., 2019).

Gráfico 1. Comparação da Taxa de Falsos Positivos



Fonte: Autores, 2026

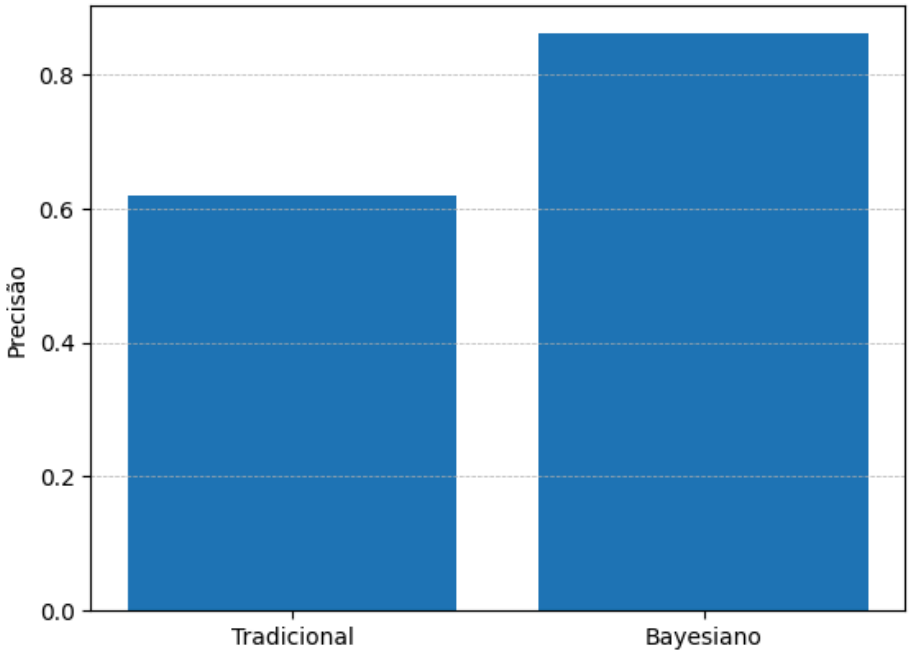
A diferença observada indica melhora significativa na filtragem de eventos irrelevantes. Segundo Bishop (2019), modelos probabilísticos reduzem classificações equivocadas ao considerar distribuições e dependências estatísticas, diferentemente de abordagens baseadas apenas em limiares fixos.

4.2. Aumento da Precisão na Classificação de Falhas

A precisão mede quantos alertas emitidos correspondem de fato a falhas confirmadas. O modelo tradicional apresentou precisão de

0,62, enquanto o modelo bayesiano atingiu 0,86. Esse ganho indica que os alertas tornaram-se mais confiáveis, diminuindo investigações desnecessárias. Modelos estatísticos aplicados a classificação costumam apresentar melhor desempenho em ambientes com variabilidade e incerteza (HASTIE; TIBSHIRANI; FRIEDMAN, 2019).

Gráfico 2. Comparação da Precisão dos Modelos



Fonte: Autores, 2026

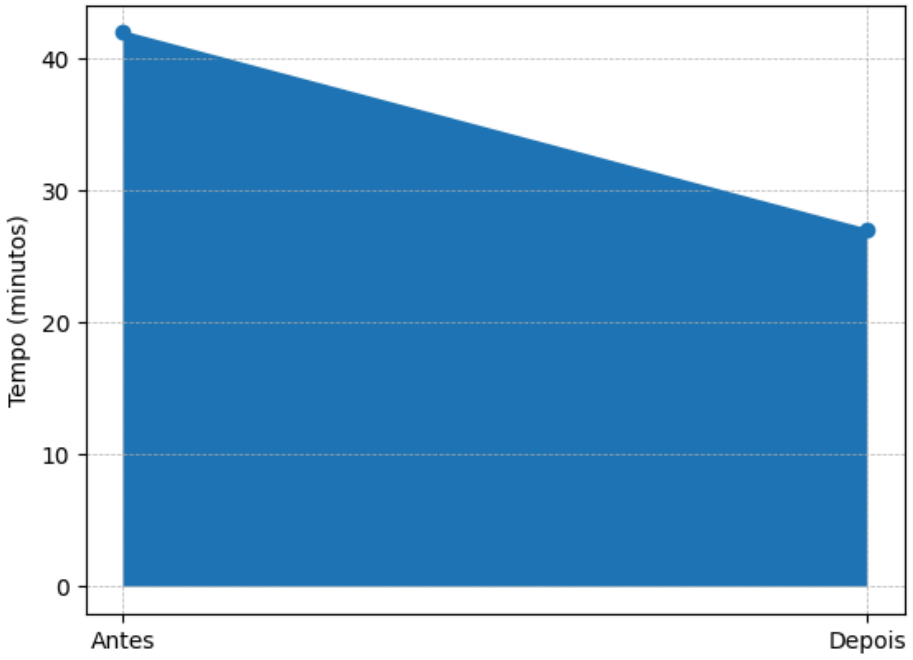
O aumento da precisão demonstra que o modelo passou a classificar eventos com maior consistência estatística. Esse resultado reforça a eficácia de métodos baseados em probabilidade para tomada de decisão sob incerteza.

4.3. Impacto no Tempo Médio de Resposta

A aplicação do modelo bayesiano produziu reflexos diretos na rotina da equipe de tecnologia da informação. Antes da implementação, o tempo médio de resposta aos incidentes considerados prioritários era de 42 minutos. Após a adoção da abordagem probabilística, esse

tempo foi reduzido para 27 minutos. Essa diferença não representa apenas um ganho numérico, mas uma mudança prática na forma como os eventos passaram a ser priorizados. Com menos alertas indevidos, a equipe conseguiu concentrar esforços em ocorrências realmente críticas, tornando o fluxo de atendimento mais objetivo e eficiente.

Gráfico 3. Evolução do Tempo Médio de Resposta (Área)



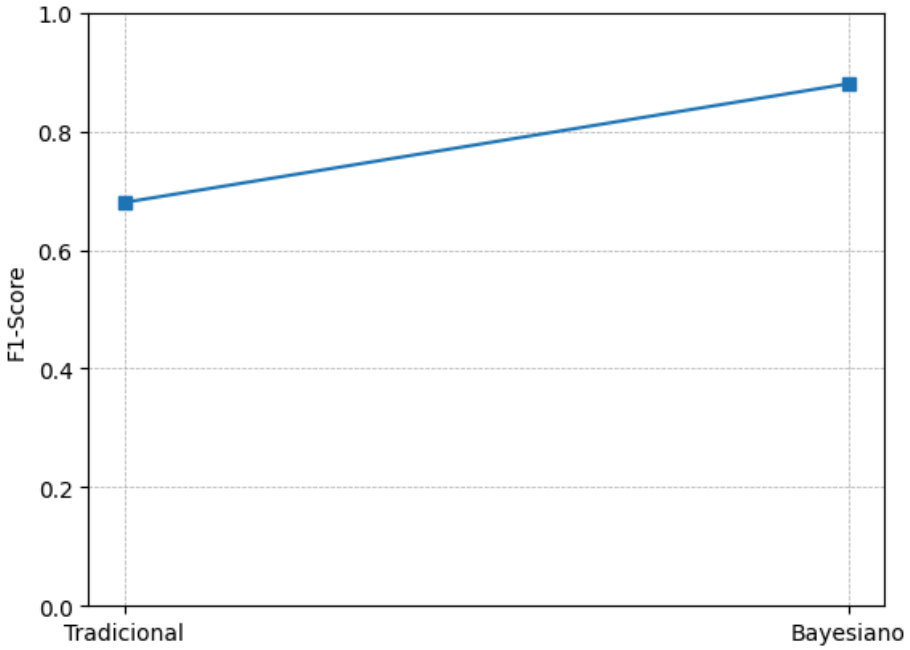
Fonte: Autores, 2026

A redução do tempo médio evidencia melhora operacional consistente, indicando que o modelo probabilístico contribuiu para decisões mais assertivas no monitoramento. Esse comportamento está alinhado com a discussão de Laprie (1992), que relaciona diretamente a confiabilidade de sistemas à capacidade de resposta eficiente diante de incidentes reais. Ao diminuir o volume de ruído no processo de detecção, o ambiente acadêmico tende a manter níveis mais elevados de disponibilidade e estabilidade.

4.4. Avaliação Global Pelo F1-score

O F1-Score foi utilizado para avaliar o desempenho geral do modelo, pois essa métrica combina precisão e revocação em um único indicador. Em cenários como a detecção de falhas, onde o número de eventos normais costuma ser muito maior do que o de falhas reais, essa medida se torna especialmente importante. O modelo tradicional apresentou F1 igual a 0,68, enquanto o modelo bayesiano alcançou 0,88. A diferença observada indica que a abordagem probabilística conseguiu manter equilíbrio entre identificar corretamente falhas reais e evitar a emissão excessiva de alertas indevidos.

Gráfico 4. Evolução Comparativa do F1-Score



Fonte: Autores, 2026

O aumento expressivo do F1-Score demonstra que o modelo bayesiano apresentou desempenho mais consistente e equilibrado. Conforme destacam Sokolova e Lapalme (2009), o F1 é uma métrica apropriada para problemas de classificação com classes desbalanceadas, pois avalia simultaneamente a capacidade de identificar corretamente eventos positivos e evitar classificações equivocadas. Assim, o resultado obtido reforça que a inferência

estatística contribui para maior estabilidade e confiabilidade no monitoramento de sistemas acadêmicos web.

5. CONSIDERAÇÕES FINAIS

Ao longo deste trabalho ficou evidente que monitorar sistemas acadêmicos web exige mais do que simplesmente configurar limites e aguardar que o sistema sinalize erros. A experiência prática demonstrou que ambientes digitais universitários são dinâmicos, variam conforme o período letivo, horários de pico e volume de acessos simultâneos. Quando o monitoramento é conduzido apenas por regras estáticas, pequenas oscilações acabam gerando interpretações equivocadas. A utilização da inferência bayesiana mostrou-se eficaz justamente por considerar o contexto e o histórico antes de classificar um evento como falha real. Com isso, foi possível reduzir ruídos, melhorar a qualidade dos alertas e tornar o processo de acompanhamento mais coerente com a realidade do sistema. A equipe técnica passou a trabalhar com informações mais confiáveis, o que impacta diretamente na organização do atendimento e na estabilidade do ambiente institucional.

Os resultados obtidos indicam que a aplicação de um modelo probabilístico não deve ser vista apenas como um recurso matemático, mas como uma mudança de perspectiva na gestão tecnológica. Quando o sistema aprende com o comportamento anterior e ajusta suas estimativas conforme novos dados surgem, o monitoramento deixa de ser reativo e passa a atuar de forma mais inteligente. Essa transformação contribui para uma infraestrutura mais resiliente e preparada para lidar com variações naturais de carga e desempenho. Ainda há espaço para evolução, como a ampliação do conjunto de variáveis analisadas e a integração com

outras técnicas analíticas, porém os achados confirmam que a inferência bayesiana representa uma alternativa consistente para fortalecer a confiabilidade e a eficiência dos sistemas acadêmicos web.

REFERÊNCIAS BIBLIOGRÁFICAS

AVIZIENIS, Algirdas et al. Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions on Dependable and Secure Computing, v. 1, n. 1, p. 11–33, 2019.

BISHOP, Christopher M. Pattern Recognition and Machine Learning. New York: Springer, 2019.

DAVIDSON-PILON, Cameron. Bayesian Methods for Hackers: Probabilistic Programming and Bayesian Inference. 1. ed. Boston: Addison-Wesley Professional, 2015.

HASTIE, Trevor; TIBSHIRANI, Robert; FRIEDMAN, Jerome. The Elements of Statistical Learning: Data Mining, Inference, and Prediction. 2. ed. New York: Springer, 2019.

LAPRIE, Jean-Claude. Dependability: Basic Concepts and Terminology. Vienna: Springer, 1992.

MARTIN, Osvaldo A.; KUMAR, Ravin; LAO, Junpeng. Bayesian Modeling and Computation in Python. 1. ed. Boca Raton: Chapman and Hall/CRC, 2021.

MARTIN, Osvaldo. Bayesian Analysis with Python. 2. ed. Birmingham: Packt Publishing Ltd., 2018.

ROUSE, Margaret. Failure Management. TechTarget, 2021. Disponível em: https://www.techtarget.com. Acesso em: 11 fev. 2026.

SANTOS, João Paulo dos. Internet das Coisas: Fundamentos, Arquiteturas e Aplicações. São Paulo: Atlas, 2019.

SOKOLOVA, Marina; LAPALME, Guy. A systematic analysis of performance measures for classification tasks. Information Processing & Management, v. 45, n. 4, p. 427–437, 2009.

STONE, James V. Bayes' Rule with Python: A Tutorial Introduction to Bayesian Analysis. 2. ed. Sheffield: Jim Stone, 2016.

TANENBAUM, Andrew S.; VAN STEEN, Maarten. Distributed Systems: Principles and Paradigms. 3. ed. Boston: Pearson, 2020.

VIEIRA, Ricardo; SOARES, Antônio Carlos. Modelagem e Simulação de Sistemas. Rio de Janeiro: LTC, 2004.

---

[1] Discente do Curso Superior de Engenharia da Computação do Centro Universitário Fametro. E-mail: acesse o artigo original para visualizar o e-mail.

[2] Mestrando em Engenharia de Processos (UFPA – PA). E-mail: acesse o artigo original para visualizar o e-mail.

[3] Especialista Instituto de Desenvolvimento Tecnológico (INDT). E-mail: acesse o artigo original para visualizar o e-mail.

[4] Doutorando em Informática pela Universidade Federal do Amazonas (UFAM). E-mail: acesse o artigo original para visualizar o

e-mail.