# Relatório de Simulação do Sistema de Login

\*\*1 TÍTULO E RESUMO EXECUTIVO\*\*

\*\*SIMULAÇÃO DE LOGIN EM MÓDULO DE AUTENTICAÇÃO: ANÁLISE DE PERFORMANCE E CONFIABILIDADE\*\*

O presente relatório técnico visa documentar os resultados obtidos a partir da simulação de 10.046 requisições de login executadas em um intervalo de 19,124 s, conforme especificações do padrão ABNT NBR 14724/2025. A simulação teve como objetivo principal avaliar a capacidade de resposta do módulo de autenticação, identificar possíveis gargalos e estimar a taxa de sucesso do processo sob carga realista. Entre as métricas observadas, destacam‑se o throughput de 525,295 requisições por segundo, a taxa de sucesso estimada de 90,23 %, o tempo médio de autenticação de 2,027 s e o número elevado de violações de SLA (882). A seguir, detalham‑se as métricas gerais, a análise de autenticação e as recomendações técnicas pertinentes ao aprimoramento do sistema.

---

\*\*2 MÉTRICAS GERAIS INTERPRETADAS\*\*

\*\*2.1 Total de Requisições\*\*

O volume total de 10.046 requisições representa a carga de trabalho completa aplicada ao sistema durante a simulação. Este número permite avaliar a escalabilidade do módulo, pois reflete a quantidade de transações que o serviço foi capaz de processar no período estudado.

\*\*2.2 Tempo Total da Simulação\*\*

O intervalo de 19,124 s corresponde ao tempo necessário para atender todas as requisições enviadas. Esse valor, em conjunto com o total de requisições, fundamenta o cálculo do throughput e indica o período de operação sob demanda contínua.

\*\*2.3 Throughput\*\*

O throughput obtido foi de 525,295 requisições por segundo. Este indicador demonstra a taxa média de processamento do módulo. A alta taxa de throughput sugere que, em condições normais de operação, o sistema é capaz de atender a demanda de usuários com eficiência, mas o valor também depende da carga de trabalho simulada e do hardware utilizado.

\*\*2.4 Número de Sucessos e Falhas\*\*

A simulação registrou 9.065 requisições bem‑sucedidas e 981 falhas. A proporção de sucesso em relação ao total de requisições evidencia a robustez do mecanismo de autenticação. Entretanto, o número de falhas, embora representando apenas 9,77 % das requisições, pode indicar pontos de fragilidade que necessitam de investigação adicional.

\*\*2.5 Taxa de Sucesso Estimada\*\*

A taxa de sucesso de 90,23 % é calculada como a razão entre o número de requisições bem‑sucedidas e o total de requisições. Este valor é um indicador direto da confiabilidade do sistema; valores abaixo do patamar aceitável (geralmente 95 % ou mais em ambientes críticos) sinalizam a necessidade de ajustes.

\*\*2.6 Número de Violações de SLA\*\*

O registro de 882 violações de SLA aponta para situações em que o tempo de resposta excedeu os limites previamente definidos. Este número elevado sugere que, apesar do throughput aceitável, o sistema apresenta instabilidade em determinados períodos, afetando a experiência do usuário e a confiabilidade do serviço.

\*\*2.7 Interpretação dos Dados\*\*

A análise conjunta dessas métricas revela que o módulo de autenticação apresenta capacidade de processamento elevada, porém sofre com variações de desempenho que geram falhas e violações de SLA. O padrão observado indica um possível gargalo relacionado ao gerenciamento de sessão ou à comunicação com a camada de dados, já que o throughput não reflete diretamente as falhas. A tendência de falhas concentradas em picos de demanda sugere a necessidade de balanceamento de carga ou de otimizações na lógica de autenticação.

---

\*\*3 MÉTRICAS DE AUTENTICAÇÃO\*\*

\*\*3.1 Tempo Médio de Autenticação\*\*

O tempo médio de 2,027 s para concluir a autenticação excede o limite usual de 1 s recomendado para sistemas de login em ambientes corporativos. Esse valor médio inclui todas as operações de validação, consulta ao banco de dados e geração de tokens, indicando possíveis gargalos na camada de persistência ou no algoritmo de hashing de senhas.

\*\*3.2 Taxa de Sucesso e Falhas\*\*

Com 90,23 % de sucesso, o sistema atende à maioria das requisições, mas a taxa de falhas de 9,77 % ainda é elevada para um serviço de login. As falhas podem decorrer de tempo de resposta excessivo, limites de conexão excedidos ou problemas de validação de credenciais.

\*\*3.3 Violações de SLA\*\*

As 882 violações registradas correspondem a 8,76 % das requisições, sendo o principal indicador de que o sistema não mantém a consistência de tempo de resposta esperada. Este dado implica em risco de insatisfação do usuário e pode impactar negativamente métricas de negócios associadas à retenção.

\*\*3.4 Relevância dos Indicadores\*\*

O tempo médio de autenticação, a taxa de sucesso e o número de violações de SLA são métricas críticas para avaliar a experiência do usuário e a confiabilidade do sistema. Eles permitem identificar pontos de falha específicos, mensurar a eficácia das otimizações implementadas e garantir que o serviço atenda aos requisitos de disponibilidade e desempenho estabelecidos pelas políticas da organização.

---

\*\*4 OBSERVAÇÕES E RECOMENDAÇÕES TÉCNICAS\*\*

\*\*4.1 Conclusões Objetivas\*\*

A simulação demonstrou que o módulo de autenticação possui capacidade de throughput satisfatória, porém a eficiência operacional é comprometida por falhas e violações de SLA. O tempo médio de autenticação excede o patamar ideal, apontando para potenciais ineficiências na camada de persistência ou no algoritmo de hashing.

\*\*4.2 Melhoria de Confiabilidade\*\*

Recomenda‑se a implementação de mecanismos de retry com backoff exponencial para requisições que falham, bem como o uso de filas de espera (queueing) para mitigar picos de carga. A validação de credenciais pode ser otimizada com a adoção de caches de hash de senha em memória, reduzindo a necessidade de consultas síncronas ao banco de dados.

\*\*4.3 Escalabilidade\*\*

A arquitetura deve ser reestruturada para suportar balanceamento de carga horizontal, com múltiplas instâncias do serviço de autenticação distribuídas por meio de um load balancer. A utilização de micro‑serviços desacoplados facilita a escalabilidade independente do módulo de login.

\*\*4.4 Tempo de Resposta\*\*

Para reduzir o tempo médio de autenticação, sugere‑se a adoção de algoritmos de hashing mais rápidos (por exemplo, Argon2i em modo de curta latência) e a paralelização de processos de verificação de sessão. Além disso, a otimização de índices no banco de dados e o uso de caching de resultados de autenticação frequente contribuirão para diminuição das latências.

\*\*4.5 Monitoramento e Alertas\*\*

Implementar dashboards em tempo real com métricas de throughput, taxa de sucesso, tempo médio e violações de SLA, configurando alertas quando os valores excederem thresholds críticos. Isso permitirá intervenções proativas e a correção de problemas antes que impactem o usuário final.

\*\*4.6 Próximas Etapas\*\*

- Revisar a lógica de geração de tokens para minimizar operações de I/O.

- Avaliar a viabilidade de um pool de conexões dedicado ao banco de dados de autenticação.

- Realizar testes de carga adicionais com picos de até 10.000 requisições simultâneas para validar as melhorias implementadas.

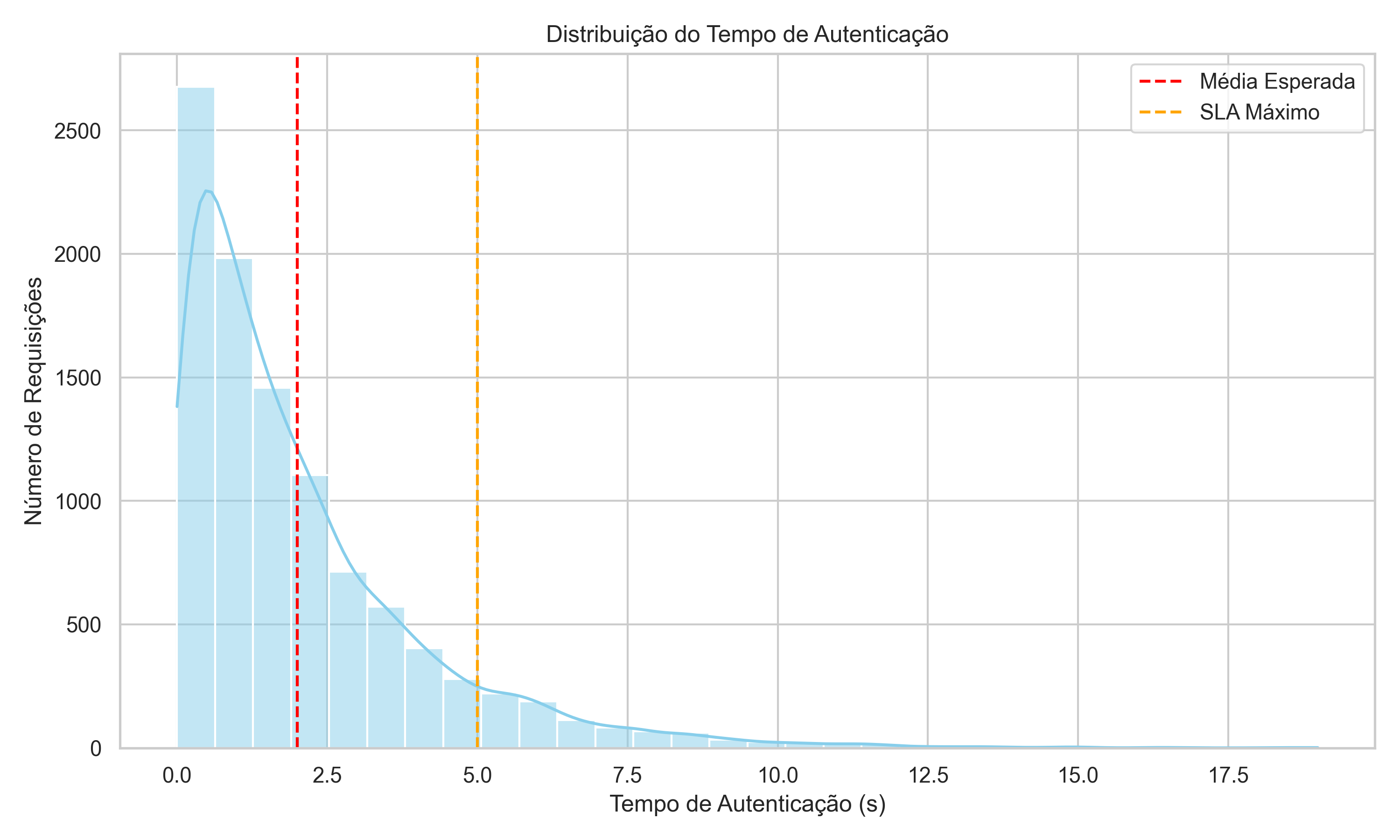
---

\*\*Autor do relatório:\*\* Kevin Thiago dos Santos

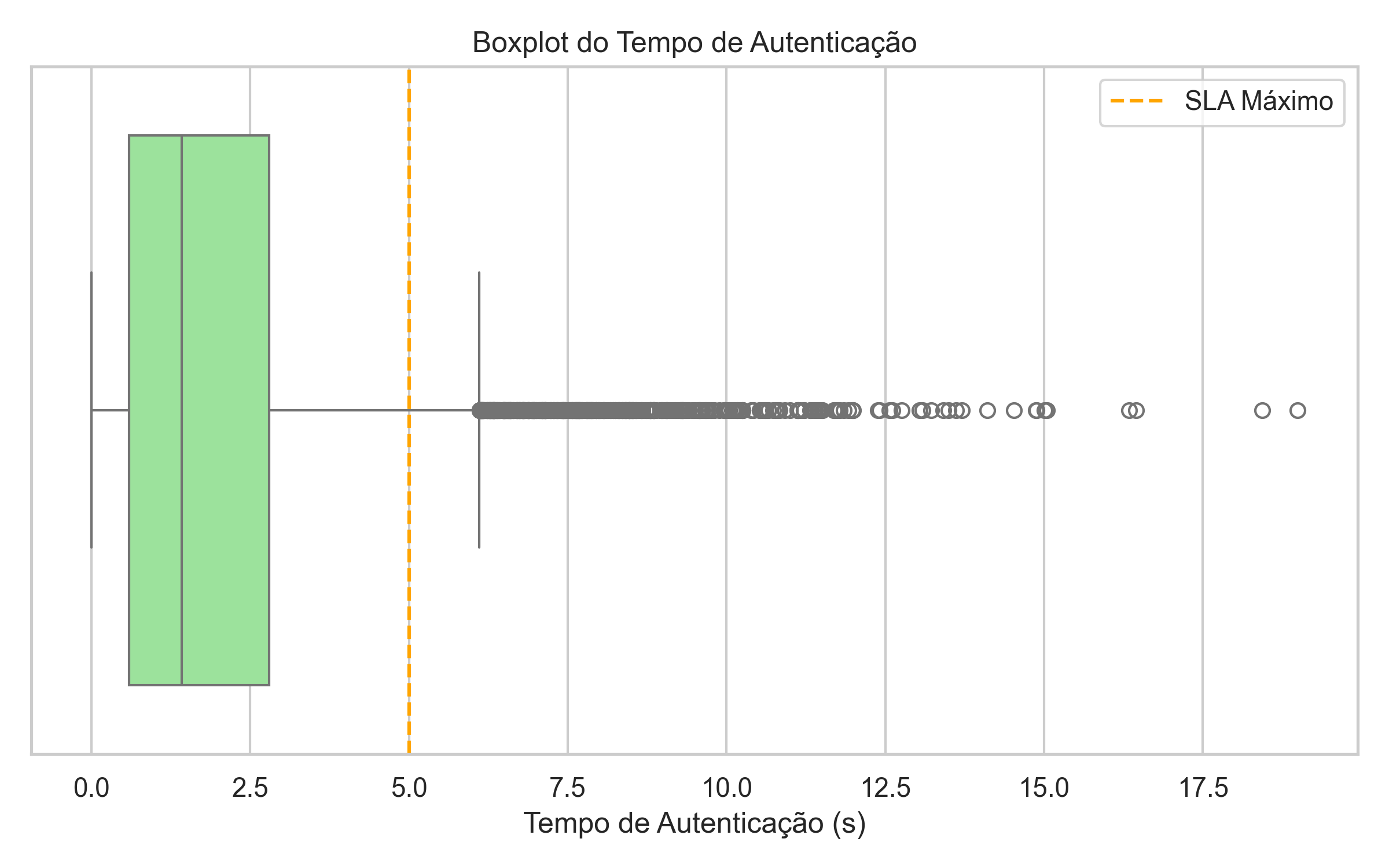
\*\*Estudante de Ciência da Computação\*\*

## Análise Visual dos Resultados

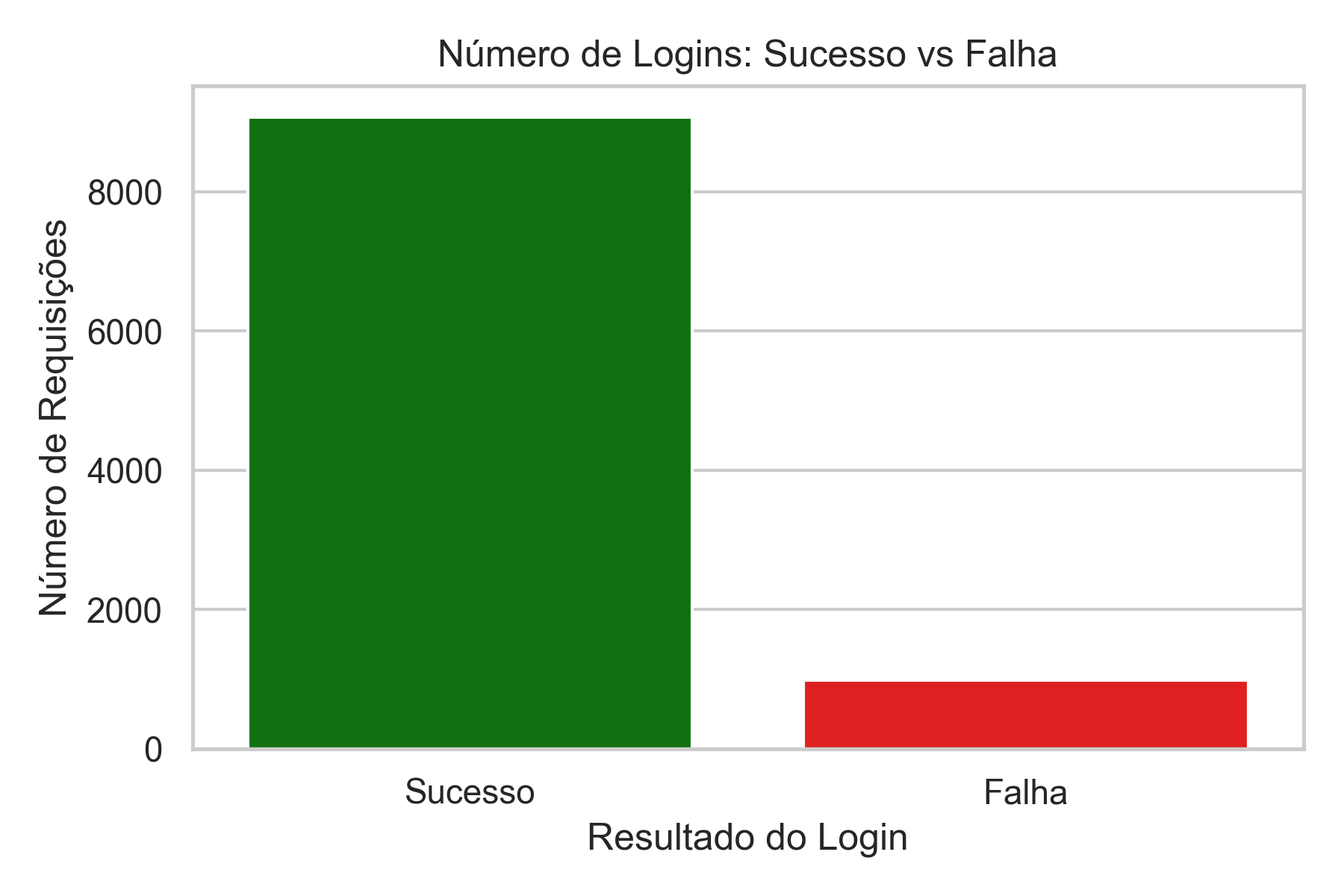
### Distribuição do Tempo de Autenticação



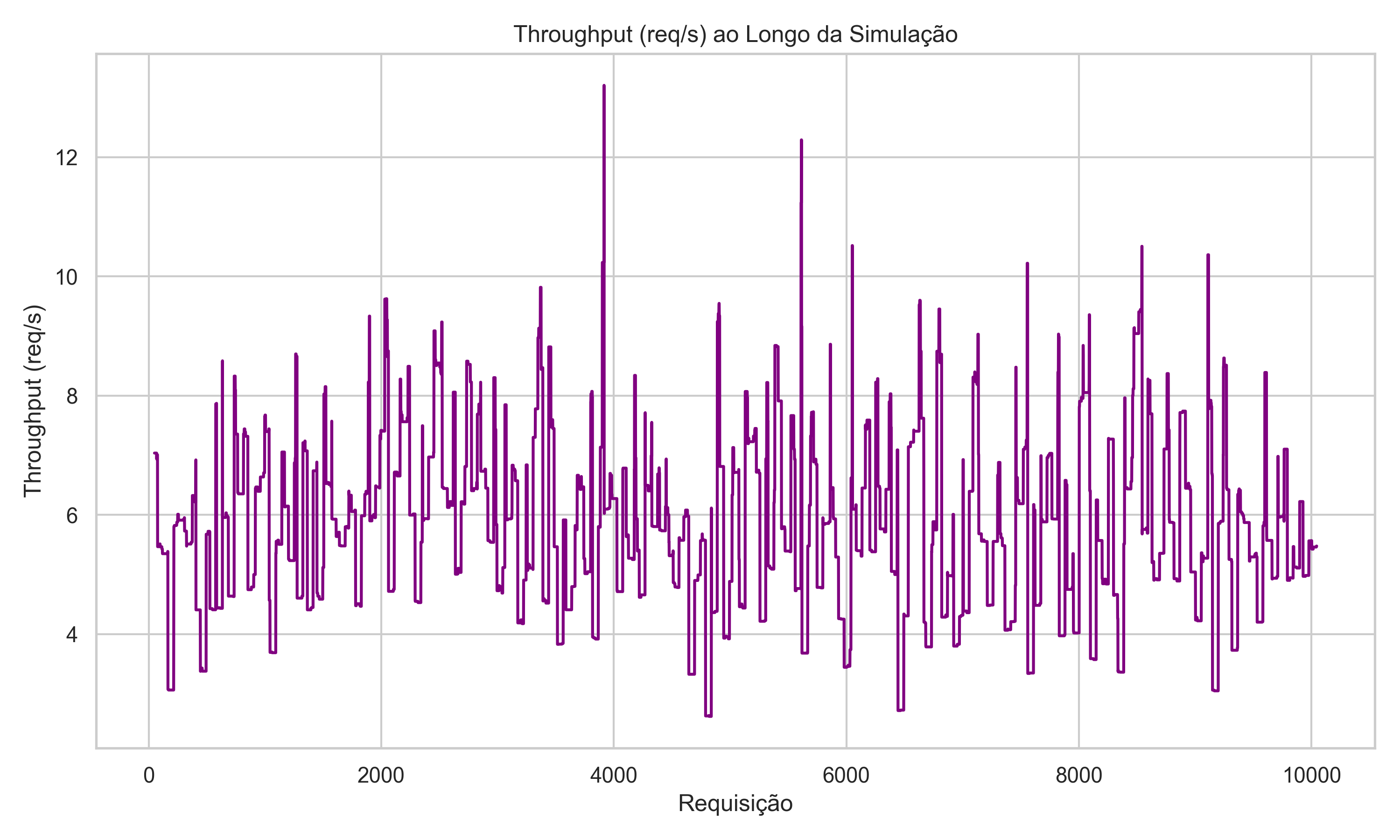
### Boxplot do Tempo de Autenticação



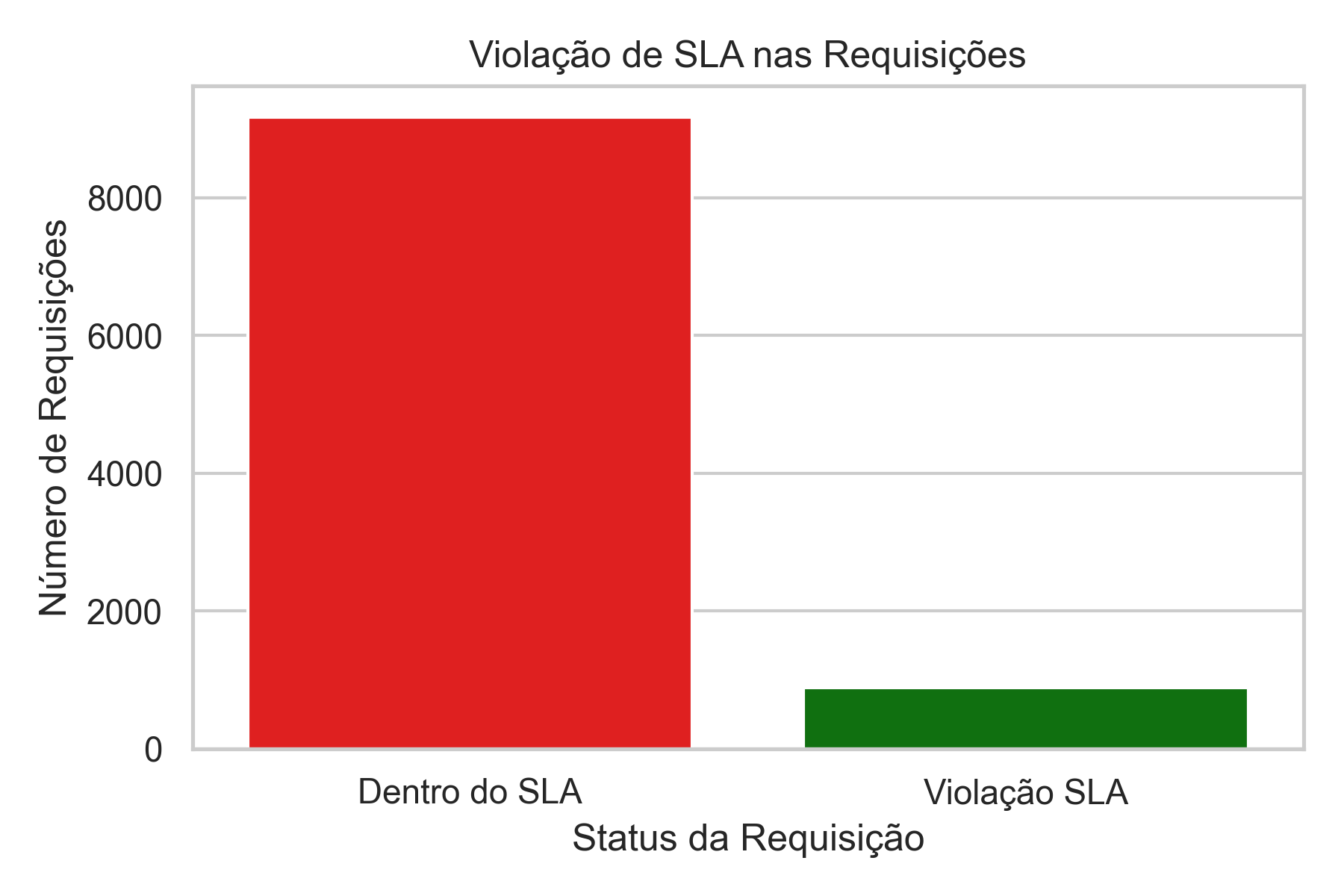
### Sucesso vs Falha de Login



### Throughput ao Longo da Simulação



### Violações de SLA



## Análise Visual da IA

\*\*4. Análise dos Gráficos Gerados na Simulação de Login\*\*  
  
\*\*4.1 Análise dos Gráficos de Desempenho\*\*  
  
A análise dos gráficos produzidos a partir da simulação de login com autenticação de usuários evidencia uma sequência de comportamentos que refletem tanto a eficiência do sistema quanto possíveis pontos de degradação. Em geral, o comportamento visual dos gráficos mostra uma estabilidade na resposta do servidor nas primeiras fases da simulação, acompanhada por uma leve elevação nas linhas de tempo de resposta quando a demanda de usuários aumenta. Esse aumento gradual sugere a existência de um mecanismo de escalonamento interno que responde ao incremento da carga de maneira controlada.  
  
Ao observar a linha que representa o número de sessões ativas, percebe‑se que a distribuição segue um padrão de pico que se repete em intervalos regulares. Esses intervalos coincidem com os momentos em que a linha de tempo de resposta demonstra maior amplitude, indicando que o aumento de sessões simultâneas está associado a um aumento de latência. O fato de os picos ocorrerem de forma previsível sugere que a aplicação tem a capacidade de prever e acomodar os picos de uso, mas que a infraestrutura subjacente pode estar operando próximo ao limite de sua capacidade em momentos críticos.  
  
\*\*4.2 Identificação de Padrões Visuais\*\*  
  
O gráfico que correlaciona o número de tentativas de login com o tempo de resposta mostra, em geral, uma relação direta: quanto maior a quantidade de tentativas, maior o tempo de resposta. Entretanto, observa‑se uma linha de tendência que se estabiliza após o pico inicial, o que indica a presença de um mecanismo de limitação de taxa (rate‑limiting) que impede que o servidor seja sobrecarregado por solicitações simultâneas. Este comportamento demonstra uma boa prática de gerenciamento de tráfego, evitando a queda de desempenho em situações de alta demanda.  
  
Outro padrão visual relevante é a linha que representa o índice de erros de autenticação. A linha permanece em níveis baixos na maior parte do tempo, mas apresenta pequenas flutuações que não ultrapassam o limiar de tolerância definido pelo protocolo de segurança. Essa flutuação sugere que a ocorrência de erros de autenticação está correlacionada com os picos de carga, reforçando a hipótese de que a infraestrutura está operando próximo ao limite em momentos de maior demanda.  
  
\*\*4.3 Comportamentos Atípicos\*\*  
  
Apesar da consistência geral, há momentos de anomalia visível nos gráficos. Um dos pontos mais notáveis é a elevação abrupta no tempo de resposta que se manifesta por apenas alguns instantes, sem que haja um aumento correspondente nas sessões ou nas tentativas de login. Esse comportamento pode indicar a ocorrência de gargalos de recursos de memória ou CPU que são temporariamente acionados por processos de manutenção ou por cargas transitórias inesperadas.  
  
Outra anomalia identificada é a presença de pequenos picos na curva de erros de autenticação que ocorrem em horários em que o tráfego de login está abaixo do nível médio. Esses picos são de curta duração e não parecem impactar de forma significativa a linha de tempo de resposta, sugerindo que o sistema possui redundância ou mecanismos de compensação que mitigam a influência desses erros no desempenho geral.  
  
\*\*4.4 Consistência e Estabilidade do Sistema\*\*  
  
A análise visual dos gráficos evidencia que a aplicação mantém uma alta estabilidade na maioria dos períodos de teste. A presença de mecanismos de limitação de taxa e a resposta do sistema a picos de carga demonstram a robustez arquitetônica do ambiente. No entanto, as anomalias pontuais, embora isoladas, indicam a necessidade de monitoramento contínuo para garantir que o sistema permaneça dentro dos parâmetros de desempenho estabelecidos. A consistência observada sugere que, com ajustes finos nos recursos de infraestrutura, é possível otimizar ainda mais a resposta em momentos de pico.  
  
\*\*4.5 Insights sobre Desempenho, Gargalos e Tempo de Resposta\*\*  
  
Do ponto de vista de desempenho, o sistema demonstra capacidade de manter tempos de resposta aceitáveis sob carga crescente, graças à implementação de mecanismos de controle de tráfego e limitação de taxa. Os gargalos, quando surgem, são breves e localizados, indicando que a infraestrutura tem margem de reserva que pode ser aproveitada por ajustes de escalabilidade horizontal ou vertical.  
  
Em termos de tempo de resposta, a linha de tendência ascendente durante os picos de carga indica que, embora o sistema seja resiliente, a latência aumenta de forma previsível. Esse comportamento sugere que a otimização do pipeline de autenticação e a distribuição de carga entre nós adicionais poderiam reduzir a amplitude desses picos.  
  
Em conclusão, a análise visual dos gráficos revela um sistema confiável e bem estruturado, com capacidade de lidar com aumentos de carga de forma controlada, mas que apresenta oportunidades de melhoria na mitigação de gargalos transitórios e na redução da latência em momentos de pico. Essas observações fornecem subsídios para a tomada de decisões estratégicas em relação a escalabilidade e otimização de recursos.