

RELATÓRIO DE INCIDENTES DE SEGURANÇA

Aplicação de Transparência – ALEPI

Período: 08/09/2026 a 13/09/2026

Aplicação: Portal da Transparência – ALEPI

Áreas envolvidas: Equipe de Tecnologia da Informação da ALEPI e TrueTec

Destinatário: Comitê de Segurança e Privacidade

1. OBJETIVO

O presente relatório tem como objetivo registrar, de forma resumida, os incidentes de segurança que afetaram a disponibilidade da aplicação de Transparência da Assembleia Legislativa do Estado do Piauí – ALEPI, ocorridos entre os dias **08/09/2026 e 13/09/2026**.

O documento apresenta a cronologia das indisponibilidades identificadas, as principais medidas adotadas pelas equipes técnicas e a evolução do comportamento do tráfego malicioso após a implementação dos mecanismos de proteção.

Para sua elaboração, foram consideradas as evidências disponíveis nos sistemas de monitoramento da infraestrutura, especialmente os registros do **Zabbix**, bem como os dados relacionados ao tráfego e aos bloqueios realizados pelos mecanismos de segurança, WAF da AWS.

Este relatório também tomou como base o documento **“Relatório Técnico de Incidente de Segurança – Ataque de Negação de Serviço Distribuída (DDoS) – Camada 7”**, confeccionado pela equipe de TI da ALEPI.

2. RESUMO DO INCIDENTE

Durante o período analisado, a aplicação de Transparência apresentou **quatro ocorrências de indisponibilidade**, associadas inicialmente a alterações indevidas em

arquivos da aplicação e, posteriormente, a um volume elevado de requisições característico de ataque de **negação de serviço distribuída (DDoS) – Camada 7**.

Os dois primeiros eventos ocorreram no dia **08/09/2026** e envolveram a alteração do arquivo index.php da aplicação. Após essas ocorrências, foram realizadas ações de contenção, incluindo revisão e restrição das permissões dos diretórios do servidor de aplicação.

No dia **10/09/2026**, ocorreu uma nova indisponibilidade associada ao elevado volume de tráfego direcionado à aplicação. A partir desse momento, a equipe de TI da ALEPI, em conjunto com a equipe técnica da TrueTec, iniciou uma atuação de resposta e mitigação, com implementação progressiva de regras e mecanismos de proteção, incluindo WAF.

Durante o processo de mitigação, o tráfego malicioso continuou sendo observado e apresentou novas rajadas de requisições. Entretanto, com a evolução das regras de proteção, o impacto sobre a disponibilidade da aplicação foi progressivamente reduzido.

3. LINHA DO TEMPO

08/09/2026 – 08:57

Primeira indisponibilidade – Injector

Às **08:57**, foi identificada a primeira indisponibilidade da aplicação.

Durante a intervenção técnica, foram identificados indícios de alteração indevida do arquivo index.php da aplicação.

A indisponibilidade teve duração aproximada de **15 minutos**, após os quais o serviço foi restabelecido.

08/09/2026 – 09:48

Segunda indisponibilidade – Injector

Às **09:48**, foi registrada uma segunda ocorrência de indisponibilidade.

Novamente foram identificados indícios de alteração do arquivo index.php.

Diante da recorrência do evento, foram realizadas ações de contenção, incluindo a revisão das permissões de acesso aos diretórios do servidor de aplicação, com o objetivo de impedir novas alterações indevidas nos arquivos da aplicação.

A indisponibilidade permaneceu por aproximadamente **3 horas e 6 minutos**, até a conclusão das principais ações de contenção e recuperação do serviço.

10/09/2026 – 16:27

Terceira indisponibilidade – Ataque DDoS

Às **16:27**, foi identificada uma terceira ocorrência de indisponibilidade.

Nesse momento, o comportamento observado passou a apresentar características compatíveis com um **ataque de negação de serviço distribuída – DDoS, em camada 7**, conforme análise técnica realizada em conjunto pelas equipes da ALEPI e da TrueTec.

A aplicação permaneceu indisponível por aproximadamente **2 horas e 20 minutos**.

Durante esse período, foram iniciadas ações de resposta, análise do tráfego e implementação de mecanismos adicionais de proteção.

10/09/2026 – 19:18

Quarta indisponibilidade – Ataque DDoS

Às **19:18**, ocorreu uma quarta indisponibilidade da aplicação durante o processo de configuração e ajuste das regras do WAF.

O serviço foi restabelecido aproximadamente **6 minutos depois**.

Após a retomada, foram mantidos o monitoramento contínuo e os ajustes das regras de proteção.

Evidência:

Hora ▾	Severidade	Hora da recuperação	Status	Informação	Host	Incidente	Duração
10-09-2026 19:18:54	☐ Alta	10-09-2026 19:24:54	RESOLVIDO		App Transparência	Foi identificado uma falha na Aplicação Transparência Incidente: avg(/App Transparencia/web.test.fail[Acessar home da Aplicação].#3)>=1 Recuperação: last(/App Transparencia/web.test.fail[Acessar home da Aplicação].#2)=0	6m
10-09-2026 16:27:42	☐ Alta	10-09-2026 18:48:08	RESOLVIDO		App Transparência	Foi identificado uma falha na Aplicação Transparência Incidente: avg(/App Transparencia/web.test.fail[Acessar home da Aplicação].#3)>=1 Recuperação: last(/App Transparencia/web.test.fail[Acessar home da Aplicação].#2)=0	2h 20m 26s
08-09-2026 09:48:41	☐ Alta	08-09-2026 12:54:56	RESOLVIDO		App Transparência	Foi identificado uma falha na Aplicação Transparência Incidente: avg(/App Transparencia/web.test.fail[Acessar home da Aplicação].#3)>=1 Recuperação: last(/App Transparencia/web.test.fail[Acessar home da Aplicação].#2)=0	3h 6m 15s
08-09-2026 08:57:38	☐ Alta	08-09-2026 09:12:38	RESOLVIDO		App Transparência	Foi identificado uma falha na Aplicação Transparência Incidente: avg(/App Transparencia/web.test.fail[Acessar home da Aplicação].#3)>=1 Recuperação: last(/App Transparencia/web.test.fail[Acessar home da Aplicação].#2)=0	15m

Figura 01 – Monitoramento Zabbix da indisponibilidade da aplicação Transparência.

4. ATUAÇÃO DAS EQUIPES TÉCNICAS

Após a identificação da segunda ocorrência de alteração indevida do arquivo index.php do Portal da Transparência, foi realizada uma análise das permissões de acesso aos arquivos da aplicação, especialmente aos arquivos com extensão .php.

A análise identificou a necessidade de tornar as permissões de acesso e escrita mais restritivas em relação à configuração anteriormente utilizada, com o objetivo de reduzir a possibilidade de novas alterações não autorizadas nos arquivos da aplicação.

Após a adequação das permissões e a realização das verificações de integridade dos arquivos da aplicação, o Portal da Transparência foi novamente disponibilizado, após um período de aproximadamente **3 horas e 6 minutos de indisponibilidade**.

Posteriormente, após a identificação do primeiro evento de **ataque de negação de serviço distribuída (DDoS)**, foi iniciada uma atuação conjunta entre a **Equipe de Tecnologia da Informação da ALEPI** e a **Equipe Técnica da TrueTec**.

A estratégia adotada consistiu no monitoramento e na análise contínua do comportamento do tráfego direcionado à aplicação, permitindo a implementação progressiva e o aprimoramento das regras e mecanismos de segurança.

Após a retomada da aplicação, novas rajadas de requisições foram registradas. À medida que novos padrões de tráfego eram identificados, mecanismos e regras de proteção foram implementados ou ajustados, buscando ampliar a capacidade de identificação e bloqueio das requisições consideradas maliciosas.

Durante o processo de mitigação, foram observados momentos pontuais de lentidão na aplicação em decorrência das novas rajadas de requisições. Entretanto, após os ajustes realizados nos mecanismos de segurança, a aplicação permaneceu disponível, mesmo diante da continuidade das tentativas de ataque.

5. EVOLUÇÃO DO ATAQUE E MITIGAÇÃO

Após a retomada da aplicação, foram observadas novas tentativas de acesso e sucessivas rajadas de requisições.

O comportamento do tráfego foi acompanhado pelas equipes técnicas e utilizado como base para o aperfeiçoamento das regras de segurança.

A partir da implementação progressiva das regras do WAF, a capacidade de bloqueio apresentou evolução significativa.

Por volta das **23:23 do dia 10/09/2026**, foi observada uma eficácia de aproximadamente **99,9% no bloqueio do padrão de tráfego identificado como malicioso**.

A partir desse momento, embora as tentativas de ataque tenham continuado, o tráfego passou a ser predominantemente bloqueado pelos mecanismos de proteção, sem provocar nova indisponibilidade da aplicação.

Evidência:

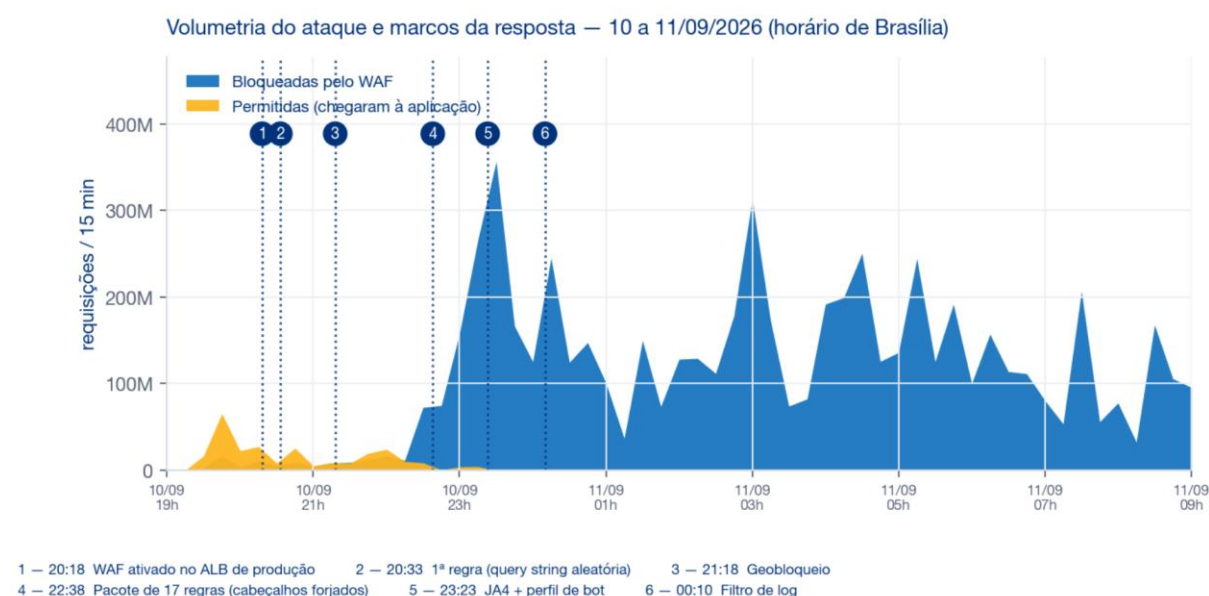


Figura 05 – Evolução do tráfego e dos bloqueios realizados pelo mecanismo de proteção.

Ao final, o ataque se resumiu nos seguintes padrões:

1.
 - a.
 - b.
2.
 - a.
 - b.
 - c.
 - d.
3.
 - a.
4.
 - a.
 - b.
5.
 - a.
 - b.
6.
 - a.

6. CONTINUIDADE DAS TENTATIVAS

As tentativas de ataque permaneceram sendo registradas após a estabilização da aplicação.

Entretanto, os mecanismos de segurança continuaram realizando o bloqueio das requisições consideradas maliciosas.

Conforme os registros analisados, o último evento relevante com volume superior a **10.000 requisições bloqueadas** ocorreu aproximadamente às **10:00 do dia 13/09/2026**.

Evidência:



Figura 06 – Evolução do tráfego e das requisições bloqueadas até 13/09/2026 WAF.

7. RESUMO DAS INDISPONIBILIDADES

Nº	Data	Horário	Evento	Duração
1	08/09/2026	08:57	Alteração indevida da aplicação	15 min
2	08/09/2026	09:48	Alteração indevida / contenção	3h06
3	10/09/2026	16:27	Ataque DDoS – Camada 7	2h20
4	10/09/2026	19:18	Ajustes das regras de WAF	6 min

Tempo total aproximado de indisponibilidade: 5 horas e 47 minutos.

8. RESULTADO DAS MEDIDAS DE SEGURANÇA

As medidas adotadas pelas equipes técnicas demonstraram evolução positiva na capacidade de proteção da aplicação.

Após a implementação e o refinamento das regras de segurança, especialmente do WAF, o volume de requisições maliciosas passou a ser bloqueado de forma significativa.

O percentual de bloqueio chegou a aproximadamente **99,9%**, reduzindo consideravelmente o impacto do ataque sobre a aplicação.

Mesmo com a continuidade das tentativas de acesso, não foram registradas novas indisponibilidades relevantes associadas ao padrão de tráfego observado após a estabilização das regras de proteção.

Dessa forma, **até o momento da elaboração deste relatório, os mecanismos de segurança implementados demonstraram-se eficazes na mitigação do padrão de ataque identificado.**

9. CONCLUSÃO

Entre os dias **08/09/2026 e 13/09/2026**, a aplicação de Transparência da ALEPI foi alvo de uma sequência de eventos de segurança que resultaram em quatro períodos de indisponibilidade.

Os dois primeiros eventos apresentaram indícios de alteração indevida do arquivo index.php, enquanto os eventos posteriores apresentaram características compatíveis com **ataque DDoS de camada 7**.

A resposta ao incidente contou com a atuação conjunta das equipes de TI da ALEPI e da TrueTec, com implementação progressiva de medidas de proteção e regras de WAF.

O acompanhamento do tráfego demonstrou que, após o processo de ajuste das proteções, a capacidade de bloqueio alcançou aproximadamente **99,9%**, permitindo que a aplicação permanecesse disponível mesmo diante da continuidade das tentativas de ataque.

Com base nas evidências disponíveis e no acompanhamento realizado até **13/09/2026**, conclui-se que as medidas de segurança implementadas foram **eficazes na mitigação do padrão de ataque observado**, mantendo a aplicação operacional após a estabilização dos mecanismos de proteção.

Em resumo: tratou-se de um ataque voltado à indisponibilidade do serviço e ao dano de imagem da instituição, e não à obtenção de dados; quanto a este evento, não foi identificado acesso ou extração de informação, e a mitigação está efetiva, com o Portal operando normalmente.

Este relatório simplifica o detalhamento e procedimentos técnicos adotados e relatados no **“Relatório Técnico de Incidente de Segurança – Ataque de Negação de Serviço Distribuída (DDoS) – Camada 7”**, elaborado pela TrueTec.

Teresina – PI, 14 de setembro de 2026.

Lucas Monteiro

Equipe Técnica de Tecnologia da Informação

Assembleia Legislativa do Estado do Piauí – ALEPI