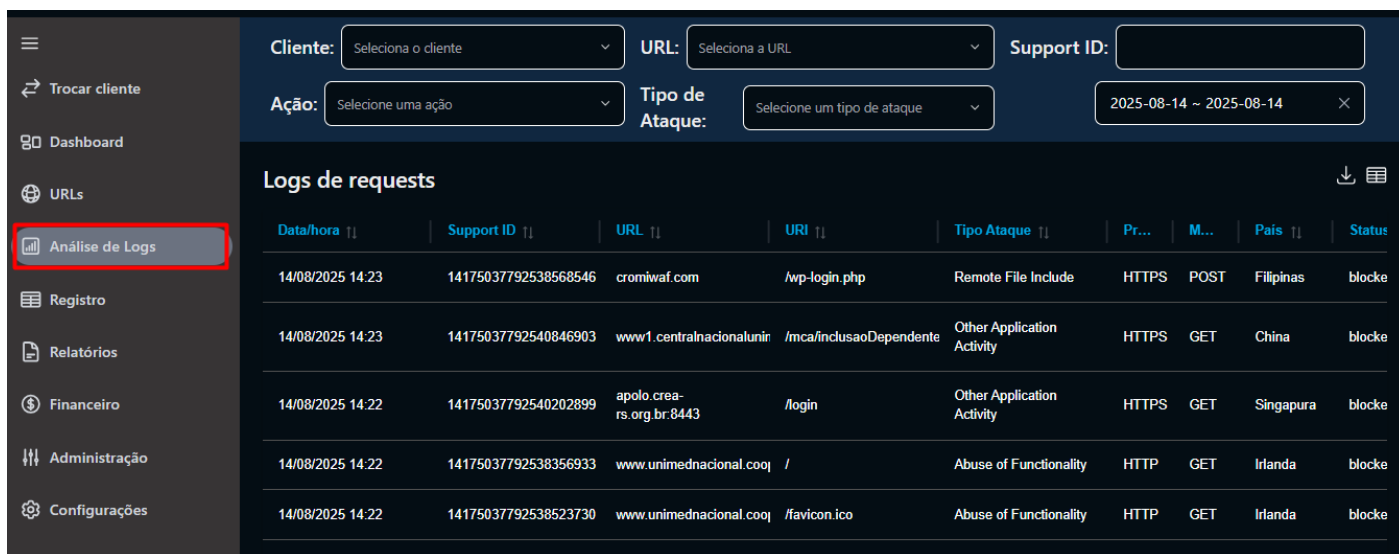


# Análise de Logs

## Guia de Uso – Análise de Logs

### 1. Acessando a tela

1. No menu lateral, clique em **Análise de Logs**.
2. A tela será carregada exibindo filtros de busca no topo e uma tabela com os logs de requisições.



The screenshot displays the 'Análise de Logs' (Log Analysis) interface. On the left, a sidebar menu contains options like 'Trocar cliente', 'Dashboard', 'URLs', 'Análise de Logs' (highlighted), 'Registro', 'Relatórios', 'Financeiro', 'Administração', and 'Configurações'. The main content area features a top section with filters: 'Cliente' (dropdown), 'URL' (dropdown), 'Support ID' (text input), 'Ação' (dropdown), 'Tipo de Ataque' (dropdown), and a date range '2025-08-14 ~ 2025-08-14'. Below the filters is a table titled 'Logs de requests' with columns: Data/hora, Support ID, URL, URI, Tipo Ataque, Pr..., M..., Pais, and Status. The table contains five rows of log entries.

| Data/hora        | Support ID           | URL                       | URI                     | Tipo Ataque                | Pr... | M... | Pais      | Status |
|------------------|----------------------|---------------------------|-------------------------|----------------------------|-------|------|-----------|--------|
| 14/08/2025 14:23 | 14175037792538568546 | cromiwaf.com              | /wp-login.php           | Remote File Include        | HTTPS | POST | Filipinas | bloque |
| 14/08/2025 14:23 | 14175037792540846903 | www1.centralnacionalunir  | /mca/inclusaoDependente | Other Application Activity | HTTPS | GET  | China     | bloque |
| 14/08/2025 14:22 | 14175037792540202899 | apolo.crea-rs.org.br:8443 | /login                  | Other Application Activity | HTTPS | GET  | Singapura | bloque |
| 14/08/2025 14:22 | 14175037792538356933 | www.unimednacional.coop   | /                       | Abuse of Functionality     | HTTP  | GET  | Irlanda   | bloque |
| 14/08/2025 14:22 | 14175037792538523730 | www.unimednacional.coop   | /favicon.ico            | Abuse of Functionality     | HTTP  | GET  | Irlanda   | bloque |

### 2. Utilizando os filtros de busca

Na parte superior, você pode filtrar os registros por:

- **Cliente** – Selecione o cliente desejado.
- **URL** – Escolha a URL associada.
- **Support ID** – Informe o identificador único da requisição.
- **Ação** – Escolha o tipo de ação executada.
- **Tipo de Ataque** – Selecione o tipo de ataque (se aplicável).
- **Período** – Selecione a data ou intervalo de datas.

Trocar cliente

Dashboard

URLs

Análise de Logs

Registro

Relatórios

Financeiro

Administração

Configurações

Cliente:

Selecione o cliente

URL:

Selecione a URL

Support ID:

Ação:

Selecione uma ação

Tipo de Ataque:

Selecione um tipo de ataque

2025-08-14 ~ 2025-08-14

×

Logs de requests

↓

☰

| Data/hora        | Support ID           | URL                      | URI                                                                          | Tipo Ataque                   | Pr... | M... | País      | Status |
|------------------|----------------------|--------------------------|------------------------------------------------------------------------------|-------------------------------|-------|------|-----------|--------|
| 14/08/2025 14:25 | 14175037792540290131 | conexaorh.sistemas.cent  | /conexaorh/ext/build/class<br>triton/resources/font-<br>ext/fonts/ExtJS.tif  | Command Execution             | HTTPS | GET  | Brasil    | bloque |
| 14/08/2025 14:25 | 14175037792542469334 | conexaorh.sistemas.cent  | /conexaorh/ext/build/class<br>triton/resources/font-<br>ext/fonts/ExtJS.woff | Command Execution             | HTTPS | GET  | Brasil    | bloque |
| 14/08/2025 14:25 | 14175037792540048164 | www.unimednacional.coq   | /                                                                            | Other Application<br>Activity | HTTP  | GET  | França    | bloque |
| 14/08/2025 14:23 | 14175037792538568546 | cromiawaf.com            | /wp-login.php                                                                | Remote File Include           | HTTPS | POST | Filipinas | bloque |
| 14/08/2025 14:23 | 14175037792540846903 | www1.centralnacionalunir | /mca/inclusaoDependente                                                      | Other Application<br>Activity | HTTPS | GET  | China     | bloque |

### 3. Interpretando a tabela de logs

A tabela apresenta as seguintes colunas:

- **Data/hora** – Momento em que a requisição foi registrada.
- **Support ID** – Identificador único da requisição.
- **URL** – Domínio ou aplicação acessada.
- **URI** – Caminho ou recurso solicitado.
- **Tipo de Ataque** – Classificação do ataque detectado.
- **Protocolo** – Ex.: HTTPS.
- **Método** – Método HTTP utilizado (GET, POST, etc.).
- **País** – Localização de origem do acesso.
- **Status** – Resultado da ação (bloqueado, alerta).
- **IP de Origem:** IP de onde foi feita a requisição.
- **Funções extras na tabela:**
  - Ícones de **seta para cima/baixo** nas colunas → permitem ordenar os registros.
  - Botão **exportar/download** (canto superior direito) → exporta os logs.
  - Botão **visualização de lista/tabela** (ao lado do exportar) → altera o layout da exibição.

Trocar cliente

Dashboard

URLs

Análise de Logs

Registro

Relatórios

Financeiro

Administração

Configurações

Cliente:

Selecione o cliente

URL:

Selecione a URL

Support ID:

Ação:

Selecione uma ação

Tipo de Ataque:

Selecione um tipo de ataque

2025-08-14 ~ 2025-08-14

×

Logs de requests

URL

URI

Tipo Ataque

Protocolo

M...

País

Status Requisição

IP de Origem

|                             |                                    |                            |      |     |                           |         |                |
|-----------------------------|------------------------------------|----------------------------|------|-----|---------------------------|---------|----------------|
| www.unimednacional.coop     | /                                  | Other Application Activity | HTTP | GET | Espanha                   | blocked | 5.135.113.20   |
| www.unimednacional.coop     | /                                  | Other Application Activity | HTTP | GET | França                    | blocked | 217.182.228.56 |
| unimednacional.coop.br      | /                                  | Other Application Activity | HTTP | GET | Alemanha                  | blocked | 18.195.122.215 |
| api-dev.unimednacional.coop | /akamai/surrogate-test-object.html | Other Application Activity | HTTP | GET | Estados Unidos da América | blocked | 23.206.202.179 |

## 4. Paginação e quantidade de registros

- Na parte inferior, é possível:
  - Escolher a quantidade de linhas por página** (ex.: 10, 25, 50...).
  - Navegar pelas páginas** usando os botões numéricos ou de avanço/retrocesso rápido.

|                          |                       |                                                                               |      |      |                           |         |                |
|--------------------------|-----------------------|-------------------------------------------------------------------------------|------|------|---------------------------|---------|----------------|
| www1.centralnacionalunir | /alfacgiapi/perl.alfa | Other Application Activity                                                    | HTTP | POST | Estados Unidos da América | blocked | 45.94.31.77    |
| www4.centralnacionalunir | /                     | Command Execution                                                             | HTTP | GET  | Estados Unidos da América | blocked | 192.53.123.118 |
| www4.centralnacionalunir | /                     | Command Execution                                                             | HTTP | GET  | Estados Unidos da América | blocked | 192.53.123.118 |
| www4.centralnacionalunir | /xmlrpc.php           | Other Application Attacks, Abuse of Functionality, Cross Site Scripting (XSS) | HTTP | POST | Lituânia                  | blocked | 91.199.163.59  |
| www4.centralnacionalunir | /xmlrpc.php           | Other Application Attacks, Abuse of Functionality, Cross Site Scripting (XSS) | HTTP | POST | Lituânia                  | blocked | 91.199.163.59  |

Linhas por página

10

1

2

3

4

5

...

2942

## 5. Exemplo de uso

- Escolha o cliente **"Exemplo"**.
- Selecione a URL **"exemplo.com"**.
- Defina o período **01/08/2025 a 14/08/2025**.
- Análise os resultados na tabela, ordenando pela coluna **Data/hora** para ver os eventos mais recentes.

Trocar cliente

Dashboard

URLs

Análise de Logs

Registro

Relatórios

Financeiro

Administração

Configurações

Cliente: CromiwafURL: cromiwaf.comSupport ID:

Ação: Seleccione uma açãoTipo de Ataque: Seleccione um tipo de ataque2025-08-01 ~ 2025-08-08

Logs de requests

Data/hora ↑Support ID ↓URL ↓URI ↓Tipo Ataque ↓Protocolo ↓M...País ↓

01/08/2025 00:2714175037792323911158cromiwaf.com/xmlrpc.phpOther Application Attacks, Abuse of Functionality, Cross Site Scripting (XSS)HTTPSPOSTAlemanha

01/08/2025 01:0314175037792324220705cromiwaf.com/xmlrpc.phpAbuse of FunctionalityHTTPSPOSTEstados Unidos da América

01/08/2025 01:051417503779232343584cromiwaf.com/xmlrpc.phpOther Application Attacks, Abuse of Functionality, Cross Site Scripting (XSS)HTTPSPOSTEstados Unidos da América

01/08/2025 01:4014175037792323481024cromiwaf.com/xmlrpc.phpOther Application Attacks, Abuse of Functionality, Cross Site Scripting (XSS)HTTPSPOSTEstados Unidos da América

Revisão #1

Criado 14 agosto 2025 17:24:22 por Leoander Neves

Atualizado: 14 agosto 2025 18:10:32 por Leoander Neves