

MANUAL API

MINDAWARE
360°

powered by **HSC**

Sumário

- **Introdução**
- **Características principais:**
- **Fluxo de Autenticação e Consumo da API HSC MindAware**
- **Dashboard do Usuário**
- **Campanhas de Comportamento**
- **Campanhas Educacionais**
- **Relatórios**
- **Códigos de Status**
- **Boas práticas**

Esse sumário deve facilitar o acesso às informações específicas.

Introdução

A API do MINDAWARE 360^a foi desenvolvida para garantir integração segura, padronizada e completa com aplicações e sistemas externos, permitindo a interoperabilidade com ambientes corporativos, plataformas de BI, sistemas de gestão e soluções de segurança da informação.

Por meio do protocolo HTTPS e da troca de informações em formato JSON, a API possibilita o consumo estruturado de dados estratégicos da plataforma, incluindo dashboards gerenciais, campanhas educacionais e comportamentais, métricas analíticas detalhadas e relatórios consolidados, assegurando confiabilidade, escalabilidade e facilidade de integração em diferentes arquiteturas tecnológicas.

Características principais:

A API do HSC MindAware 360° permite integração completa com aplicativos externos através do protocolo HTTPS, retornando dados no formato JSON. Esta API fornece acesso a dashboards, campanhas educacionais e comportamentais, métricas detalhadas e relatórios estratégicos.

A API do HSC MindAware 360° segue o padrão REST (Representational State Transfer), uma arquitetura amplamente utilizada para desenvolvimento de APIs web que oferece simplicidade, escalabilidade e padronização.

Características principais:

- **Protocolo HTTP/HTTPS:** Todas as comunicações utilizam o protocolo HTTPS seguro
- **Métodos HTTP padrão:**
 - GET para consultar dados
 - POST para criar recursos ou executar ações
 - Operações são identificadas claramente pelo método HTTP utilizado
- **Formato JSON:** Todas as requisições e respostas utilizam o formato JSON (JavaScript Object Notation)
- **Stateless:** Cada requisição é independente e contém todas as informações necessárias (incluindo o token de autenticação)
- **Endpoints baseados em recursos:** URLs organizadas de forma hierárquica e intuitiva (ex: `/api/my_dashboard/user_info`)
- **Códigos de status HTTP:** Respostas utilizam códigos HTTP padrão (200 para sucesso, 401 para não autorizado, 404 para não encontrado, etc.)

Fluxo de Autenticação e Consumo da API HSC MindAware.

1. Autenticação (Login)

- O cliente envia as credenciais de acesso (por exemplo, e-mail/usuário e senha) para o endpoint:

`POST /api/auth/login`

- Em caso de sucesso, a API retorna um **token de acesso** (JWT ou similar), que será utilizado para autenticação nas próximas requisições.

2. Autorização com Token (Bearer)

- A cada requisição a endpoints protegidos, o cliente deve incluir o token no cabeçalho HTTP:

`Authorization: Bearer <token>`

- Sem esse cabeçalho, as requisições a recursos protegidos serão negadas.

3. Requisição aos Endpoints da API

- O cliente realiza chamadas HTTP (GET, POST, PUT, DELETE, etc.) para os endpoints desejados (dashboards, campanhas, métricas, relatórios, etc.), sempre incluindo o token de acesso quando o recurso exigir autenticação.

4. Processamento no Servidor

- O servidor recebe a requisição e **valida o token** informado no cabeçalho.
- Caso o token seja válido, o servidor processa a operação solicitada (consulta, criação, atualização, etc.) e prepara a resposta correspondente.

5. Resposta da API

- Em caso de sucesso, o servidor retorna os dados solicitados em **formato JSON**, seguindo o modelo definido para cada endpoint.
- Em situações de erro (token inválido ou expirado, credenciais incorretas, ausência de permissão, erros de validação, etc.), a API responde com **códigos de status HTTP**

apropriados (como 400, 401, 403, 404, 500) e mensagens de erro padronizadas.

6. Logout e Encerramento de Sessão

- Quando o cliente desejar encerrar a sessão, pode invalidar o token chamando o endpoint:

POST /api/auth/logout

- Após o logout, o token deixa de ser aceito, exigindo um novo processo de login para voltar a consumir os recursos protegidos da API.

Esta arquitetura permite que qualquer linguagem de programação ou ferramenta que suporte HTTP possa integrar facilmente com a plataforma HSC MindAware.

Pré-requisitos

- Conta ativa no HSC MindAware 360° com privilégios administrativos
- Usuário criado e ativado no sistema
- Token de autenticação válido para chamadas protegidas

URL Base

```
1 {{url}}/api
2
```

Autenticação

Todas as rotas marcadas como "Requer Token" necessitam do token de autenticação no cabeçalho da requisição.

Login

Obtém o token de acesso para realizar chamadas autenticadas à API.

Endpoint: POST /auth/login

Requer Token: Não

Request Body:

```
1 {
2   "email": "usuario@empresa.com",
3   "password": "senha_seguza"
4 }
5
```

Response:

```

1 {
2   "access_token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1b290IjoiYm9keSIsImV4cCI6MTYxOTQ0MDAwfQ.eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1b290IjoiYm9keSIsImV4cCI6MTYxOTQ0MDAwfQ",
3   "token_type": "bearer",
4   "expires_in": 7200,
5   "user": {
6     "id": 123,
7     "name": "João Silva",
8     "email": "usuario@empresa.com"
9   },
10  "company": {
11    "id": 1,
12    "name": "Empresa XYZ"
13  },
14  "module": {},
15  "two_factor_confirmed": 0
16 }
17

```

Logout

Invalida o token de acesso atual.

Endpoint: POST /auth/logout

Requer Token: Sim

Response:

```
1 {
2   "message": "Usuário desconectado com sucesso!"
3 }
```

Formato do Header de Autenticação

Para todas as requisições que requerem autenticação, inclua o token no cabeçalho:

```
1 Authorization: Bearer <seu_token_aqui>
2
```

Dashboard do Usuário

O Dashboard do Usuário fornece uma visão consolidada das informações pessoais, progresso educacional, scores de comportamento e campanhas ativas.

- Obter Dados Completos do Dashboard

Endpoint: GET /auth/my-dashboard/{id?}

Requer Token: Sim

Parâmetros:

- id (opcional): ID do usuário. Se omitido, retorna dados do usuário autenticado.

Response:

```
1 {
2   "success": true,
3   "data": {
4     "quadrantPosition": {
5       "x": 85,
6       "y": 98
7     },
8     "certifications": [
9       {
10        "id": 1,
11        "name": "Cyber Security Awareness",
12        "completed": true,
13        "date": "2025-01-15"
14      }
15    ]
16  }
17 }
```

- Informações Básicas do Usuário

Endpoint: GET /my_dashboard/user_info/{id?}

Requer Token: Sim

Response:

```
1 {
2   "thumbnail": "...",
3   "name": "João Silva",
4   "mail": "joao@empresa.com",
5   "groups": ["Grupo A", "Grupo B", "TI"]
6 }
7 }
```


- Percentual de Cursos Concluídos

Endpoint: GET /my_dashboard/completed_course/{id?}

Requer Token: Sim

Response:

```
1 80
2
```

- Percentual de Certificações Concluídas

Endpoint: GET /my_dashboard/completed_certification/{id?}

Requer Token: Sim

Response:

```
1 60
2
```

- Score Educacional

Retorna o score atual do usuário baseado no progresso educacional.

Endpoint: GET /my_dashboard/edu_score/{id?}

Requer Token: Sim

Response:

```
1 95
2
```

- Score de Comportamento Seguro

Retorna o score de comportamento baseado nas campanhas de simulação.

Endpoint: GET /my_dashboard/comp_score/{id?}

Requer Token: Sim

Response:

```
1 88
2
```

- Gráfico de Evolução de Scores

Retorna dados históricos para visualização da evolução dos scores educacional e comportamental.

Endpoint: GET /my_dashboard/edu_comp_graph/{id?}

Requer Token: Sim

Response:

```
1 {
2   "xList": ["01/01/25", "02/01/25", "03/01/25", "04/01/25"],
3   "edu": [80, 85, 90, 95],
4   "comp": [90, 88, 92, 88]
5 }
6
```

- Progresso Detalhado dos Cursos

Endpoint: GET /my_dashboard/course_progress/{id?}

Requer Token: Sim

Response:

```
1 [
2 {
3   "id": 1,
4   "name": "Cyber Security Awareness Essentials",
5   "progress": 90,
6   "course_structure": [
7     {
8       "id": 101,
9       "name": "Módulo 1: Fundamentos",
10      "progress": 100,
11      "course_content": [
12        { "id": 1001, "name": "Introdução à Segurança" },
13        { "id": 1002, "name": "Ameaças Comuns" }
14      ]
15    },
16    {
17      "id": 102,
18      "name": "Módulo 2: Phishing",
19      "progress": 80,
20      "course_content": [
21        { "id": 1003, "name": "Reconhecendo Phishing" },
22        { "id": 1004, "name": "Estudos de Caso" }
23      ]
24    }
25  ],
26  "course_certification": [
27    {
28      "id": 1,
29      "name": "Certificação Básica",
30      "status": "pending"
31    }
32  ],
33  "totalConteudos": 10
34 }
35 ]
```

- Campanhas Ativas do Usuário

Endpoint: GET /my_dashboard/campaigns/{id?}

Requer Token: Sim

Response:

```
1 [
2 {
3   "id": 123,
4   "name": "Campanha Anti-Phishing Q1 2025",
5   "type": "behavioral",
6   "status": "active",
7   "date_start": "2025-01-10",
8   "date_end": "2025-03-31",
9   "progress": 45
10 }
11 ]
12
```

Campanhas de Comportamento

As Campanhas de Comportamento permitem simulações de phishing e outros ataques para testar e treinar usuários em cenários reais.

- Listar Todas as Campanhas

Endpoint: GET /company_campaigns/

Requer Token: Sim

Response:

```
1 {
2   "campaigns": [
3     {
4       "id": 1,
5       "name": "Campanha de Phishing - Q1 2025",
6       "date_start": "2025-01-15 00:00:00",
7       "date_end": "2025-03-31 23:59:59",
8       "custom_template": 0,
9       "step_count": 3,
10      "mail_from": "noreply@phishing-test.com",
11      "mail_subject": "Atualização Urgente de Segurança",
12      "mail_body": "...",
13      "name_template": "Phishing Financeiro",
14      "description_template": "Simulação de email de banco fraudulento",
15      "thumbnail_template": "https://...",
16      "campaign_categories_id": 2,
17      "webpage_body": "...",
18      "trigger_time": 1,
19      "trigger_schedule": "[{"date": "2025-01-15/01/2025", "hour": "09:00"}, {"date": "2025-02-15/02/2025", "hour": "14:00"}]",
20      "landing_page": "https://landing.mindaware.com/campaign1",
21      "date_close": "2025-04-10",
22      "created_at": "2025-01-10 10:30:00",
23      "updated_at": "2025-01-12 15:20:00",
24      "deleted_at": null
25    }
26  ]
27 }
28
```

- Detalhes da Campanha

Retorna informações completas sobre uma campanha específica.

Endpoint: GET /company_campaigns/campaigns_details/{id_campanha}

Requer Token: Sim

Response:

```

1 {
2   "campaigns": {
3     "id": 1,
4     "name": "Campanha de Phishing - Q1 2025",
5     "total_users": 250,
6     "date_start": "2025-01-15",
7     "date_end": "2025-03-31"
8   },
9   "count_templates": {
10    "phishing": 5,
11    "smishing": 2,
12    "vishing": 1
13  },
14  "triggers": [
15    {
16      "id": 1001,
17      "user_id": 50,
18      "status": "email_opened",
19      "timestamp": "2025-01-15 09:15:23"
20    }
21  ],
22  "triggers_history": [
23    {
24      "trigger_id": 1001,
25      "status": "sent",
26      "timestamp": "2025-01-15 09:00:00"
27    },
28    {
29      "trigger_id": 1001,
30      "status": "opened",
31      "timestamp": "2025-01-15 09:15:23"
32    }
33  ]
34 }
35

```

- Relatório PDF da Campanha

Gera um relatório estratégico em PDF da campanha.

Endpoint: GET /company_campaigns/campaigns_details_pdf/{id_campanha}

Requer Token: Sim

Response:

```

1 {
2   "pdf": "JVBERi0xLjcKCjEgMCBvYmoKPDMKLR5cGUgL0NhZdGFsb2cKL18hZ2VzIDIgMCBSCj4+CnVuZG91agoKMl..."
3 }
4

```

- Métricas de Disparos

Retorna métricas percentuais dos disparos por status.

Endpoint: GET

/company_campaigns/triggersByCampaignWithPercent/{id}/{status?}

Requer Token: Sim

Parâmetros:

- `id`: ID da campanha
- `status` (opcional): Filtrar por status específico

Status disponíveis:

- pending - E-mail pendente
- sent - E-mail enviado
- opened - E-mail aberto
- clicked - Link clicado
- submitted - Dados submetidos
- canceled - Cancelado

Response:

```
1 {  
2   "percent": 75.5  
3 }  
4
```

- Log dos Disparos por Usuário

Endpoint: POST /company_campaigns/triggersDetailsByUser/{id_campanha}

Requer Token: Sim

Response:

```
1 [  
2   {  
3     "picture": "https://cdn.mindaware.com/avatars/user50.jpg",  
4     "name": "Maria Santos",  
5     "mail": "maria.santos@empresa.com",  
6     "category": "Phishing",  
7     "template": "Phishing Financeiro",  
8     "status": "Link clicado",  
9     "timestamp": "2025-01-15 09:15:23"  
10  },  
11  {  
12    "picture": "https://cdn.mindaware.com/avatars/user51.jpg",  
13    "name": "João Silva",  
14    "mail": "joao.silva@empresa.com",  
15    "category": "Phishing",  
16    "template": "Phishing Corporativo",  
17    "status": "E-mail aberto",  
18    "timestamp": "2025-01-15 09:28:45"  
19  }  
20 ]  
21
```

- Histórico Detalhado do Disparo

Retorna o histórico completo de um disparo específico, incluindo dados técnicos quando disponíveis.

Endpoint: GET /company_campaigns/getTriggerHistory/{id_trigger}

Requer Token: Sim

Response:

```

1 [
2   {
3     "id": 1001,
4     "timestamp": "2025-01-15 09:00:00",
5     "status": 1,
6     "status_name": "E-mail enviado"
7   },
8   {
9     "id": 1001,
10    "timestamp": "2025-01-15 09:15:23",
11    "status": 2,
12    "status_name": "E-mail aberto",
13    "ip": "192.168.1.100",
14    "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64)...",
15    "location": "São Paulo, BR"
16  },
17  {
18    "id": 1001,
19    "timestamp": "2025-01-15 09:16:18",
20    "status": 3,
21    "status_name": "Link clicado",
22    "ip": "192.168.1.100",
23    "browser": "Chrome 128.0",
24    "os": "Windows 10"
25  }
26 ]
27

```

- Datatable de Disparos

Endpoint otimizado para exibição em tabelas com suporte a pesquisa avançada.

Endpoint: GET /company_campaigns/datatableTriggers?id={id_campanha}

Requer Token: Sim

Query Parameters (filtros opcionais):

- date_trigger - Data do disparo (formato: YYYY-MM-DD)
- user - Nome do usuário
- mail - E-mail do usuário
- template - Nome do template/categoria
- status - Status do disparo

Exemplo de URL com filtros:

```

1 /company_campaigns/datatableTriggers?id=1&user=João&status=clicado
2

```

Response:

```

1 {
2   "aaData": [
3     {
4       "__timestamp": "2025-01-15 09:00:00",
5       "__name": "João Silva",
6       "__mail": "joao.silva@empresa.com",
7       "__template": "Phishing Básico",
8       "__status": "E-mail aberto",
9       "__user_id": 50
10    },
11    {
12      "__timestamp": "2025-01-15 09:05:00",
13      "__name": "Maria Santos",
14      "__mail": "maria.santos@empresa.com",
15      "__template": "Phishing Financeiro",
16      "__status": "Link clicado",
17      "__user_id": 51
18    }
19  ]
20 }
21

```

Campanhas Educacionais

As Campanhas Educacionais gerenciam treinamentos, cursos e certificações dos usuários.

- Detalhes da Campanha Educacional

Endpoint: GET /training_company_campaigns/details/{id_campanha}

Requer Token: Sim

Response:

```
1 {
2   "success": true,
3   "data": {
4     "id": 1,
5     "name": "Treinamento de Segurança Q1 2025",
6     "description": "Programa completo de conscientização em segurança da informação",
7     "certification": 1,
8     "date_start": "2025-01-10",
9     "date_end": "2025-03-31",
10    "total_users": 150,
11    "courses": [
12      {
13        "id": 1,
14        "name": "Cyber Security Awareness Essentials"
15      },
16      {
17        "id": 2,
18        "name": "Advanced Phishing Detection"
19      }
20    ]
21  }
22 }
23 }
```

- Métricas da Campanha Educacional

Retorna métricas específicas baseadas no tipo e status solicitados.

Endpoint: GET /training_company_campaigns/{type}/{status}/{id_campanha}

Requer Token: Sim

Parâmetros:

- **type:**
 - `metric` - Retorna objeto com numerador e denominador
 - `count` - Retorna apenas o valor numérico
- **status:**
 - `opened` - E-mails abertos
 - `clicked` - Links clicados
 - `course_initiated` - Cursos iniciados
 - `course_completed` - Cursos concluídos

- `cert_pending` - Certificações pendentes
- `cert_completed` - Certificações concluídas
- `users` - Total de usuários

Response (type="metric"):

```
1 {
2   "triggers": 25,
3   "total": 50
4 }
5
```

Response (type="count"):

```
1 25
2
```

Exemplos de uso:

```
1 GET /training_company_campaigns/metric/course_completed/1
2 GET /training_company_campaigns/count/users/1
3
```

- Relatório Detalhado CSV

Gera relatório detalhado em formato CSV/JSON com todos os dados dos usuários.

Endpoint: POST

`/training_company_campaigns/trainingCampaignCsv/{id_campanha}`

Requer Token: Sim

Response:

```
1 [
2   {
3     "training_camp_name": {
4       "name": "Treinamento de Segurança Q1 2025"
5     },
6     "Nome": "João Silva",
7     "Email": "joao.silva@empresa.com",
8     "Grupo": "TI",
9     "Iniciaram curso": 2,
10    "Concluíram curso": 1,
11    "Certificação pendente": 0,
12    "Certificação concluída": 1,
13    "Data último acesso": "2025-01-15 14:30:00"
14  },
15  {
16    "training_camp_name": {
17      "name": "Treinamento de Segurança Q1 2025"
18    },
19    "Nome": "Mazia Santos",
20    "Email": "maria.santos@empresa.com",
21    "Grupo": "RH",
22    "Iniciaram curso": 1,
23    "Concluíram curso": 0,
24    "Certificação pendente": 0,
25    "Certificação concluída": 0,
26    "Data último acesso": "2025-01-14 10:15:00"
27  }
28 ]
29
```

- Relatório Estratégico PDF

Gera relatório executivo em PDF da campanha educacional.

Endpoint: GET /training_company_campaigns/pdf/{id_campanha}

Requer Token: Sim

Response:

```
1 {
2   "pdf": "JVBER10xLjcKCjEgMCBvYm9KP0wKL1R5cGUGL0Nh0Fsb2cKL1BhZ2VzIDIGMCBSCj4+CnVuZ691agoKMi..."
3 }
4
```

Log dos Disparos (Datatable)

Retorna dados formatados para exibição em tabelas com informações dos disparos educacionais.

Endpoint: GET

/training_company_campaigns/datatableTriggers?id={id_campanha}

Requer Token: Sim

Query Parameters (filtros opcionais):

- name - Nome do usuário
- mail - E-mail do usuário
- date_trigger - Data do disparo
- status - Status do progresso

Response:

```
1 {
2   "aData": [
3     {
4       "id": 123,
5       "training_camp_id": 1,
6       "user_id": 456,
7       "timestamp": "2025-01-10 09:00:00",
8       "name": "João Silva",
9       "mail": "joao.silva@empresa.com",
10      "courses": [
11        "Cyber Security Awareness Essentials",
12        "Advanced Phishing Detection"
13      ],
14      "status": 5,
15      "status_name": "Curso concluído"
16    },
17    {
18      "id": 124,
19      "training_camp_id": 1,
20      "user_id": 457,
21      "timestamp": "2025-01-10 09:05:00",
22      "name": "Maria Santos",
23      "mail": "maria.santos@empresa.com",
24      "courses": [
25        "Cyber Security Awareness Essentials"
26      ],
27      "status": 4,
28      "status_name": "Curso iniciado"
29    }
30  ]
31 }
32
```

- Histórico do Usuário na Campanha

Retorna o histórico completo de progresso de um usuário específico em uma campanha educacional.

Endpoint: GET

/training_company_campaigns/getTriggerHistory/{user_id}/{id_campanha}

Requer Token: Sim

Response:

```
1 [
2   {
3     "status": 1,
4     "status_name": "E-mail enviado",
5     "timestamp": "2025-01-10 09:00:00"
6   },
7   {
8     "status": 2,
9     "status_name": "E-mail aberto",
10    "timestamp": "2025-01-10 09:15:00"
11  },
12  {
13    "status": 3,
14    "status_name": "Link clicado",
15    "timestamp": "2025-01-10 09:20:00"
16  },
17  {
18    "status": 4,
19    "status_name": "Curso iniciado",
20    "timestamp": "2025-01-10 09:25:00"
21  },
22  {
23    "status": 5,
24    "status_name": "Curso concluído",
25    "timestamp": "2025-01-12 14:30:00"
26  },
27  {
28    "status": 7,
29    "status_name": "Certificação concluída",
30    "timestamp": "2025-01-12 15:00:00"
31  }
32 ]
33
```

Relatórios

- Relatório de Métricas Educacionais

Gera relatório completo com dados educacionais de todos os usuários.

Endpoint: POST /reports/users_courses

Requer Token: Sim

Response:

```

1 [
2 {
3   "name": "João Silva",
4   "mail": "joao.silva@empresa.com",
5   "type": "USER",
6   "groups": "TI, Segurança",
7   "certification": "Sim",
8   "certification_date": "2025-01-12",
9   "course_name": "Cyber Security Awareness Essentials",
10  "course_status": "Concluido",
11  "course_start_date": "2025-01-10",
12  "course_end_date": "2025-01-12",
13  "has_completed": true
14 },
15 {
16   "name": "Maria Santos",
17   "mail": "maria.santos@empresa.com",
18   "type": "USER",
19   "groups": "RH",
20   "certification": "Não",
21   "certification_date": null,
22   "course_name": "Cyber Security Awareness Essentials",
23   "course_status": "Em Andamento",
24   "course_start_date": "2025-01-10",
25   "course_end_date": null,
26   "has_completed": false
27 },
28 {
29   "name": "Carlos Oliveira",
30   "mail": "carlos.oliveira@empresa.com",
31   "type": "USER",
32   "groups": "Grupo TODOS",
33   "certification": "Não",
34   "certification_date": null,
35   "course_name": "Cyber Security Awareness Essentials",
36   "course_status": "Não Iniciado",
37   "course_start_date": null,
38   "course_end_date": null,
39   "has_completed": null
40 }
41 ]
42

```

- Relatório de Métricas de Comportamento

Retorna dados comportamentais baseados nas campanhas de simulação.

Endpoint: POST /company_campaigns/triggersDetailsByUser/{id_campanha}

Requer Token: Sim

Response:

```

1 [
2 {
3   "campaign_name": "Campanha Anti-Phishing Q1",
4   "user_name": "João Silva",
5   "mail": "joao.silva@empresa.com",
6   "category": "Phishing",
7   "template": "Phishing Financeiro",
8   "status": "Link clicado",
9   "timestamp": "2025-01-15 09:16:10"
10 },
11 {
12   "campaign_name": "Campanha Anti-Phishing Q1",
13   "user_name": "Maria Santos",
14   "mail": "maria.santos@empresa.com",
15   "category": "Phishing",
16   "template": "Phishing Corporativo",
17   "status": "E-mail aberto",
18   "timestamp": "2025-01-15 09:20:45"
19 }
20 ]
21

```

Códigos de Status

- Status de Campanhas Comportamentais

Código	Status	Descrição
0	Pendente	E-mail pendente de envio
1	E-mail enviado	E-mail foi enviado com sucesso
2	E-mail aberto	Usuário abriu o e-mail
3	Link clicado	Usuário clicou no link do e-mail
4	Dados submetidos	Usuário submeteu dados no formulário
5	Cancelado	Disparo foi cancelado

- Status de Campanhas Educacionais

Código	Status	Descrição
0	E-mail pendente	E-mail aguardando envio
1	E-mail enviado	E-mail foi enviado
2	E-mail aberto	Usuário abriu o e-mail
3	Link clicado	Usuário acessou o link do treinamento

4	Curso iniciado	Usuário iniciou o curso
5	Curso concluído	Usuário completou o curso
6	Certificação pendente	Aguardando aprovação da certificação
7	Certificação concluída	Certificação obtida com sucesso

- Status de Cursos

Status	Descrição
Não Iniciado	Curso ainda não foi acessado
Em Andamento	Curso iniciado mas não concluído
Concluído	Curso finalizado com sucesso
Expirado	Prazo de conclusão expirou

Boas Práticas

Segurança

- Nunca exponha o token em logs, URLs ou código cliente
- Renove o token antes da expiração (válido por 7200 segundos / 2 horas)
- Valide sempre as respostas da API antes de processar

Performance

- Cache tokens válidos para evitar logins repetidos
- Utilize filtros nos endpoints de datatable para reduzir payload
- Reutilize conexões HTTP quando possível

Tratamento de Erros

A API utiliza códigos HTTP padrão para indicar o sucesso ou falha das requisições:

- **200 OK:** Requisição processada com sucesso
- **401 Unauthorized:** Token expirado ou inválido
- **403 Forbidden:** Sem permissão para acessar o recurso
- **404 Not Found:** Recurso não encontrado
- **500 Internal Server Error:** Erro interno do servidor

Sempre valide o código de status HTTP antes de processar a resposta.

Material exclusivo da
HSC, referente ao
MindAware 360°.

Copyright © 2025 HSC.
Não copie sem permissão.



hsclabs.com

+55 51 3500 8255