



Design de APIs Fantásticas

Fabio Biasi Mello Rubim

#37

Embarcadero Conference 2019

Da sala de reunião à vida real

- Desenvolvedor Delphi há mais de 8 anos
- Desenvolvedor sênior na Embarcadero Professional Services
- Graduado em Análise e Desenvolvimento de Sistemas pela Fatec Sorocaba
- Pós-graduando em Engenharia de Software pela Unicamp



Qual escolher?

#37

SOAP ou REST

XML ou JSON



- É um protocolo

Prós:

- Padrão bem definido pela indústria (governo, instituições financeiras)
- Bem documentado
- Pode utilizar vários protocolos para o transporte

Contras:

- Utiliza somente XML
- “Verboso”
- Difícil de compreender
- Um pouco mais lento do que REST

- É uma arquitetura

Prós:

- Utiliza o protocolo HTTP
- Simples de compreender
- Utiliza JSON, XML...entre outros
- Mais rápido que SOAP
- Aprendizado mais rápido
- Menos padronizado

Contras:

- Menos padronizado

SOAP + REST? Confuso?

- Lembra SOAP/RPC
 - Mas... utiliza POST!
 - POST em sua maioria:
 - Por exemplo:
 - Vai alterar alguma coisa, POST
 - Vai deletar alguma coisa, POST
 - Vai criar um novo recurso, POST (no mínimo, né?!)

flickr.photos.notes.add
flickr.photos.notes.delete
photos.notes.edit

flickr.photos.comments.add
flickr.photos.comments.delete
flickr.photos.comments.deleteCoords
flickr.photos.comments.edit
flickr.photos.comments.get
flickr.photos.comments.getList

Como utilizar REST ou ser RESTful

REST: Representational State Transfer.

- Estilo arquitetural criado por Roy Fielding.
- Existem basicamente dois “entendimentos” sobre o que é ser *RESTful*:
 - O modo acadêmico, como descrito na tese de doutorado de Roy Fielding
 - O “resumido” ou de “mercado”



Como utilizar REST ou ser RESTful

Modo acadêmico:

- **Uniform interface:** Deve possuir uma interface, URI, que identifique unicamente o recurso e seja acessível do mesmo modo a qualquer cliente
- **Client-server architecture:** Clara separação entre quem efetua as requisições e quem recebe e executa as requisições
- **Stateless:** Cada nova requisição deve conter os dados necessários para a mesma. Quem gerencia o estado é a aplicação cliente.
- **Cacheability:** Se os dados da resposta não mudarem, não será necessário processar novamente a requisição.
- **Layered system:** Permite uma arquitetura em camadas, onde você tem sua API no servidor A, seus dados no servidor B e a autenticação no servidor C.
- **Code on demand (opcional):** A resposta de uma requisição pode ser um código que execute algo em seu cliente, ou seja, não somente conteúdo estático.

Como utilizar REST ou ser RESTful

O utilizado pelo mercado:

- ***Uniform Interface***: URI que identifique unicamente um recurso
- **Utilizar os verbos HTTP para as ações de Create, Read, Update e Delete:**
 - **C**: Post para criar um recurso
 - **R**: Get para obter um recurso
 - **U**: Put para atualizar um recurso
 - **D**: Delete para excluir um recurso



Como utilizar REST ou ser RESTful

Resource	POST(Create) C	GET(Read) R	PUT(Update,Create) U	Delete(Delete) D
/clientes	Cria um novo recurso, no caso um novo cliente.	Lista dos clientes.	-----	Exclui todos os clientes. Não é comum a sua utilização.
/clientes/8974	-----	Exibe o somente um recurso, neste caso o cliente “8974”.	Atualiza o cliente “8974”, caso o mesmo não exista, é criado.	Exclui somente o cliente “8974”.

- Composição de uma **URI**:

- **http://api[minhaempresa].com.br/nome-da-api/recurso**

HTTP ou
HTTPS

Seu domínio

Nome da API
(opcional)

Recursos e
parâmetros

Boas práticas – *Resource*, singular ou plural?

- ~~/cliente:~~
- */clientes*: Geralmente representam um *array*, podendo retornar zero, um ou muitos itens.

```
{[]}
```

Boas práticas – *Cacheable, Safe e Idempotent*

- ***Safe***: São métodos HTTP que não alteram o estado do servidor. Efetuam somente a leitura do recurso.
- ***Idempotent***: São métodos que recebem inúmeras requisições e o resultado permanece o mesmo, o servidor não muda o seu estado. **Levando em consideração que os métodos foram implementados de forma correta.**
- ***Cacheable***: São métodos que utilizam cache.

Boas práticas – *Cacheable, Safe e Idempotent*

- **GET (Cacheable, Safe, Idempotent):**
 - GET /clientes/896541/enderecos
 - GET /checklist/item/2
- **Não faça:** GET /checklist/item/**DELETE/2** - Deixou de ser safe, idempotente e cacheable

Boas práticas – *Cacheable, Safe e Idempotent*

- **POST (Unsafe, Not-Idempotent):**

- ```
POST /clientes/8974/enderecos
{
 "endereco": "Av. das Nações Unidas",
 "numero": "13797",
 "complemento": "7º andar – Conjunto Morumbi",
 "bairro": "Vila Gertrudes",
 "cidade": "São Paulo",
 "estado": "SP",
 "cep": "04794-000"
}
```

# Boas práticas – *Cacheable, Safe e Idempotent*

- **PUT (Unsafe, Idempotent):**

- `PUT /clientes/8974/enderecos/1`  
`{`  
    `"endereco": "Av. das Nações Unidas",`  
    `"numero": "13797", t`  
    `"complemento": "7º andar – Conjunto Morumbi ",`  
    `"bairro": "Vila Gertrudes",`  
    `"cidade": "São Paulo",`  
    `"estado": "SP",`  
    `"cep": "04794-000"`  
`}`

# Boas práticas – *Cacheable, Safe e Idempotent*

- **DELETE (Unsafe, Idempotent):**
  - [DELETE /clientes/8974/enderecos/1](#)

# Boas práticas – *Cacheable, Safe e Idempotent*

- **PATCH (Unsafe, Not-Idempotent):**

- PATCH /clientes/8974/endereços/1

{

"endereço":"Av. Paulista"

}

# Boas práticas – UUID como identificador

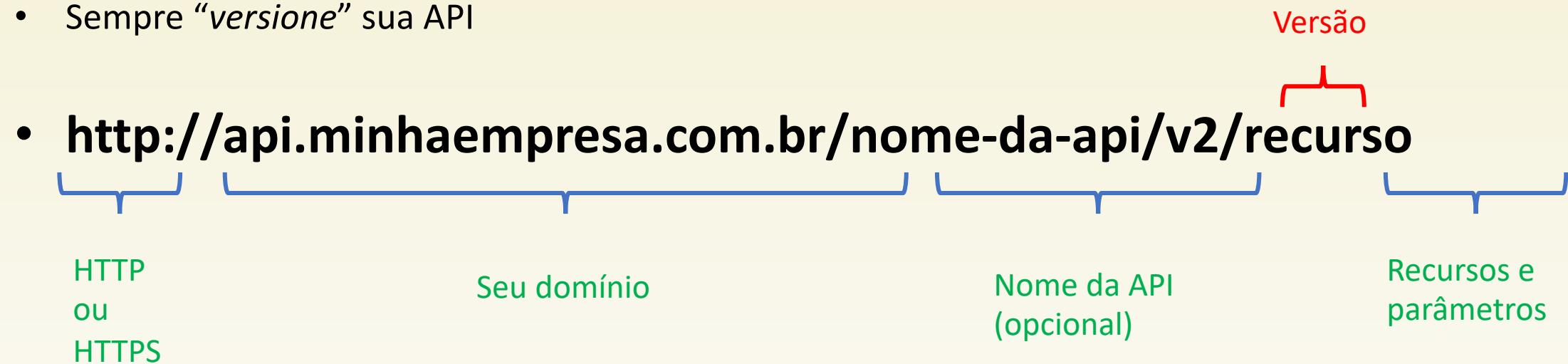
- Se houver padrão, pode ser inseguro
  - Fácil alterações dos dados
  - Bots, scrapping e etc
- Identificador universal e exclusivo
  - Algo como: 0092f377-15ef-48ca-8b3a-b9faba415780
  - Ex: [http://api\[minhaempresa\].com.br/clientes/0092f377-15ef-48ca-8b3a-b9faba415780](http://api[minhaempresa].com.br/clientes/0092f377-15ef-48ca-8b3a-b9faba415780)
  - Sem hifens: [http://api\[minhaempresa\].com.br/clientes/0092f37715ef48ca8b3ab9faba415780](http://api[minhaempresa].com.br/clientes/0092f37715ef48ca8b3ab9faba415780)

# Boas práticas – UUID como identificador

- **Vantagens:**
  - Esconde a quantidade de registros
  - Dificulta a manipulação da URI
- **Desvantagens:**
  - Complicado ao depurar
  - Maior espaço de armazenamento
  - Menor desempenho

- **NUNCA quebre o cliente**

- Sempre “*versione*” sua API



Outras alternativas:

- Twilio: `/2018-04-01/Accounts/`
- Salesforce.com: `/services/data/v20.0/limits`

- Padrão de 3 dígitos que indica o resultado da requisição
  - XXX
- Divididos em 5 classes, identificadas pelo primeiro dígito
  - 1xx – 2xx – 3xx – 4xx – 5xx
- Os *clients* não precisam lidar com todos os códigos, mas sim as classes e alguns códigos mais importantes

# Boas práticas – Status Codes

- **1xx: Informational**
  - Resposta informando que o servidor recebeu a requisição e está processando a mesma
  - 100: Continue
  - 101: Switching Protocols
  - 102: Processing (WebDAV)

# Boas práticas – Status Codes

- **2xx: Successful**

- **200 OK:** Status genérico de sucesso. Normalmente usado como resposta a GETs ou atualizações com PUT/PATCH.
- **201 CREATED:** Indica que um recurso foi criado. Normalmente usado para responder a requisições com PUTs e POSTs.
- **202 ACCEPTED:** Indica que a requisição foi aceita para processamento. Normalmente utilizada em chamadas assíncronas.
- **204 NOT CONTENT:** A requisição obteve sucesso, mas não há nada para mostrar. Normalmente usada como resposta a DELETEs.
- **206 PARTIAL CONTENT:** O retorno está incompleto. Normalmente usado em recursos com paginação.

# Boas práticas – Status Codes

- 3xx :
  - Responsável por efetuar vários tipo de redirecionamentos
    - 300: Multiple choices
    - 301: Moved Permanently
    - 302: Found

# Boas práticas – Status Codes

- **4xx : Client Error**
  - **400 BAD REQUEST:** Status genérico de erro para requisições que não puderam ser processadas.
  - **401 UNAUTHORIZED:** O servidor não reconheceu você por falta de credenciais válidas para o recurso solicitado.
  - **403 FORBIDDEN:** Sua credencial não tem privilégios suficientes para acessar o recurso que está solicitando.
  - **422 UNPROCESSABLE ENTITY:** Ocorreu algum erro de negócio com sua mensagem. Sintaticamente correto, semanticamente não.

# Boas práticas – Status Codes

- **4xx : Client Error**
  - **413 ENTITY TOO LARGE:** A requisição que você está enviando é excede o limite que o servidor é capaz de processar.
  - **429 TOO MANY REQUESTS:** O servidor está limitando o seu acesso por que você atingiu o limite máximo de requisições.
  - **404 NOT FOUND:** Indica que o servidor não encontrou o recurso destino identificado na requisição. Pode não ser um estado permanente -- que seria indicado por 410 (Gone).
  - **415 UNSUPPORTED MEDIA TYPE:** O payload está em um formato que o servidor não reconhece. As vezes é resolvido com os atributos Content-Type ou Content-Encoding.

- **5xx : Successful**

- **500 INTERNAL SERVER ERROR:** A requisição está certa, porém algum erro aconteceu no servidor. Não adianta mandar de novo agora!
- **503 SERVICE UNAVAILABLE:** O servidor não consegue processar agora por sobrecarga ou manutenção.

# Boas práticas – Status Codes - BÔNUS

- **418**

- É um código de erro HTTP para o cliente
- **418 I'm a teapot** indica que o servidor se recusa a preparar café por ser um bule de chá. Este erro é uma referência ao **Hyper Text Coffee Pot Control Protocol**, que foi uma piada de 1º de abril de 1998.

Fonte: <https://tools.ietf.org/html/rfc2324>



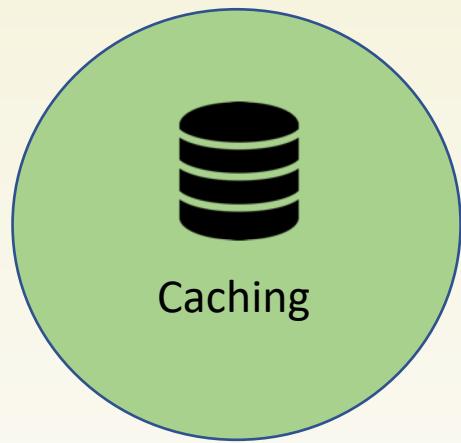
# Boas práticas – Status Codes - Segurança

- Uma boa prática é retornar um **404** toda vez que ocorre um **401** ou **403**.

- **401 UNAUTHORIZED:** O servidor não reconheceu você por falta de credenciais válidas para o recurso solicitado.
- **403 FORBIDDEN:** Sua credencial não tem privilégios suficientes para acessar o recurso que está solicitando.



Filtro e  
Paginação



Caching



Callback

- **Busca global:**
- **GET /search?q=comida+italiana**



- **Busca com escopo (subconjuntos):**
- **GET**  
`/vendas/v2/pedidos?status=concluido`

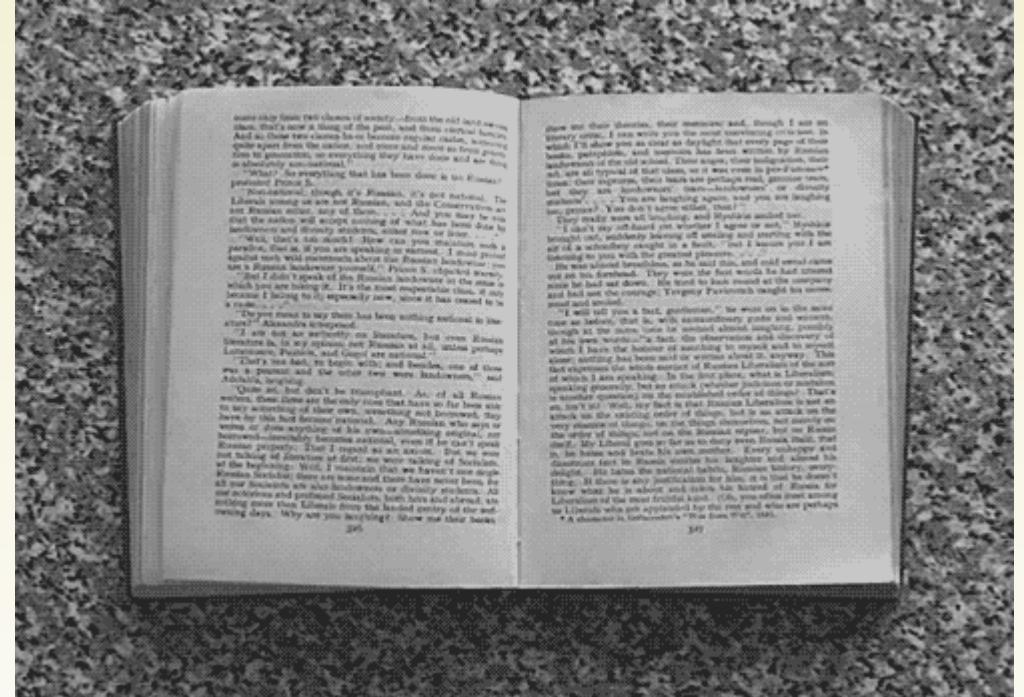


- **Respostas parciais**
- **GET**  
`/pedidos/9640E7...?_fields=numero,data,valor`



# Boas práticas – Paginação

- Recomendação:
- GET  
**/pedidos?\_offset=50&\_limit=25**



# Boas práticas – Paginação

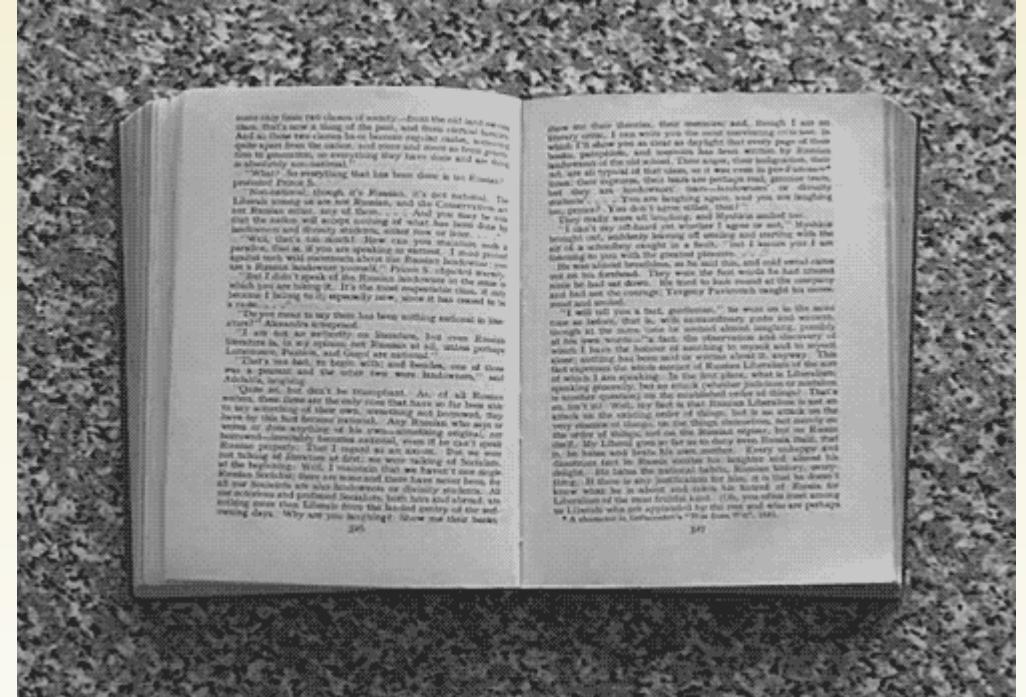
- Recomendação:
- Outras opções:

• [Linkedin: ?start=50&count=25](#)

• [Instagram:](#)

?min\_id=3091&max\_id=3245&coun

t=25



# Boas práticas – Documentação - Swagger

- EndPointRequestSummary

```
[EndPointRequestSummary('ATags', 'ASummary', 'ADescription', 'AProduces', 'AConsume')]
```

- EndPointRequestParameter

```
[EndPointRequestParameter('AIn', 'AName', 'ADescription', 'ARequired', 'AType', 'AFormat', 'AltemType',
'AJSONSchema', 'AReference')]
```

- EndPointResponseDetails

```
[EndPointResponseDetails('ACode', 'ADescription', 'AType', 'AFormat', 'ASchema', 'AReference')]
```

# Boas práticas – Documentação - Swagger

- [EndPointObjectsYAMLDefinitions](#)

```
[EndPointObjectsYAMLDefinitions(Objects)]
```

- [EndPointObjectsJSONDefinitions](#)

```
[EndPointObjectsJSONDefinitions(Objects)]
```

- RAD Server URLs

- <http://localhost:8080/api/apidoc.yaml>
- <http://localhost:8080/api/apidoc.json>

# Boas práticas – Documentação - Swagger

Swagger Editor. Supported by SMARTBEAR

```

1 swagger: '2.0'
2 info:
3 description: Api Documentation
4 version: '1.0'
5 title: Api Documentation
6 termsOfService: 'urn:tos'
7 contact: {}
8 license:
9 name: Apache 2.0
10 url: 'http://www.apache.org/licenses/LICENSE-2.0'
11 host: 'localhost:8080'
12 basePath: /
13 tags:
14 - name: basic-error-controller
15 description: Basic Error Controller
16 - name: events-controller
17 description: 'Set of endpoints for Creating, Retrieving, Updating and Deleting of Events.'
18 - name: guests-controller
19 description: 'Set of endpoints for Creating, Retrieving, Updating and Deleting of Guests for events.'
20 - name: hosts-controller
21 description: 'Set of endpoints for Creating, Retrieving, Updating and Deleting of Hosts.'
22 - name: invitation-controller
23 description: 'Set of endpoints for Creating, Retrieving, Updating and Deleting of Events invitations.'
24 paths:
25 /api/v1/events:
26 get:
27 tags:
28 - events-controller
29 summary: Get all events by host id
30 operationId: getEventsByHostIdUsingGET

```

**Sample Tag**

GET /test Summary Title

Get Method Description

Parameters

Try it out

| Name                         | Description        |
|------------------------------|--------------------|
| X-Embarcadero-Application-Id | string<br>(header) |
| X-Embarcadero-App-Secret     | string<br>(header) |
| X-Embarcadero-Master-Secret  | string<br>(header) |

Responses Response content type application/json

| Code | Description |
|------|-------------|
| 200  | Ok          |

- Evite tráfego desnecessário
- Menos latência de rede
- Menos sobrecarga nos servidores
- Atenção
  - Tempo de invalidação no cache
  - Sincronização em clusters



# Boas práticas – Callback

- **Chamadas reversas:**
  - Consulta estoque
  - Cálculo de frete
  - Novo pedido recebido

Exemplo:

`POST / api.meumarketplace.com/v1/pedido?callbackURL=https://api.meumarketplace.com/v1/estoque`

`https://api.meumarketplace.com/v1/estoque`

`https://api.meumarketplace.com/v1/frete`

`https://api.meumarketplace.com/v1/pedido`



# Boas práticas – Segurança

- Quantidade de acessos?
- Quais clientes acessam as APIs?
- Acesso a informações sensíveis?
- As APIs alteram dados importantes?

# Boas práticas – Segurança

- Autenticação autorização
  - Acesso não autorizado
  - Ataque de força bruta
  - Roubo de credenciais
  - Session hijacking
- Integridade
  - Injection (SQL, XML, JSON)
  - Cross-site scripting (XSS) e Request Forgery (XSRF)

# Boas práticas – Segurança

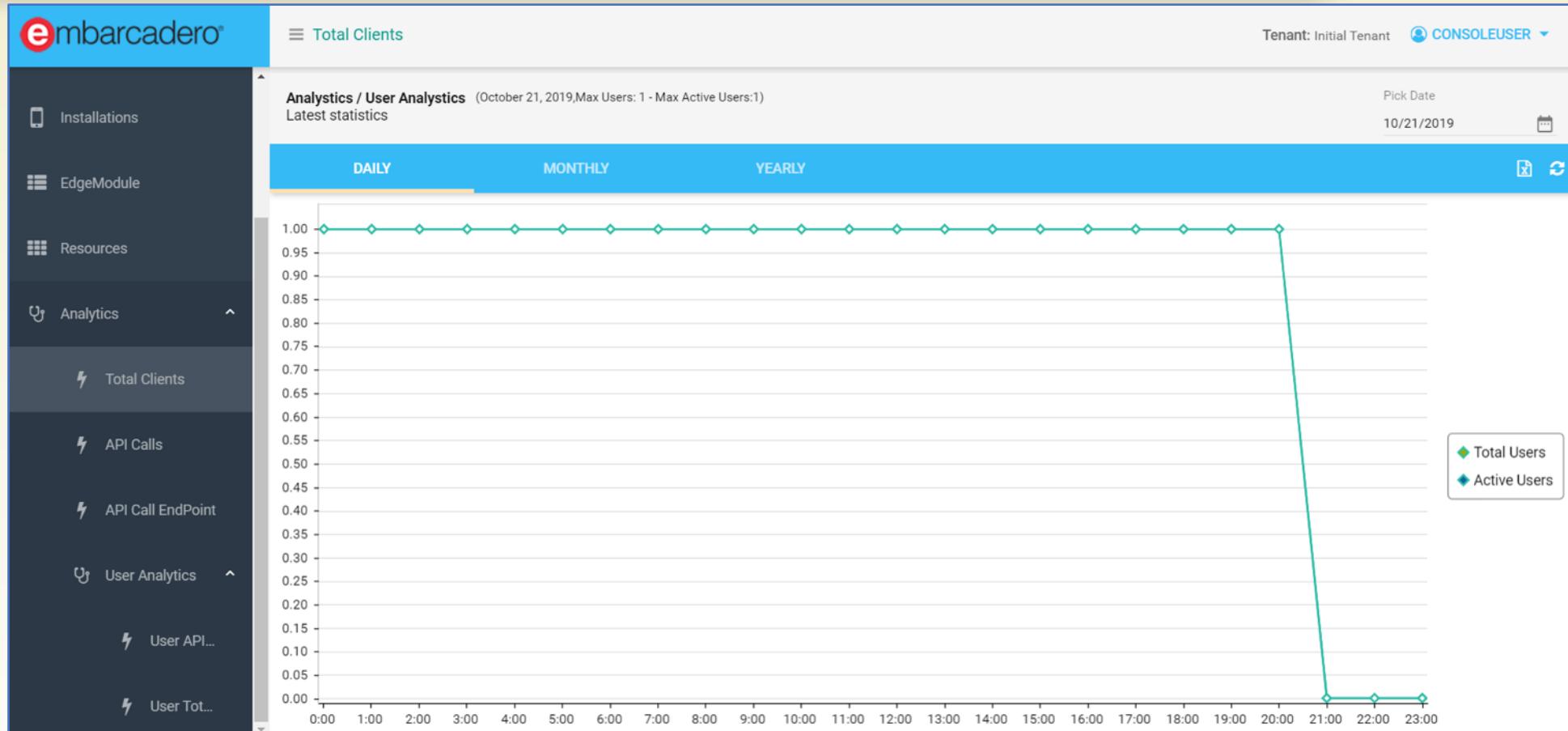
- Auditoria
  - Repudiação
  - Compliance (PCI-DSS, HIPAA)
- Disponibilidade
  - DDoS
  - Buffer overflow
  - Injection (SQL, XML, JSON)
- Privacidade
  - Information disclosure
  - Man-in-the-middle e Network eavesdropping
  - Data scrapping

# Boas práticas – Padrões de utilização

The screenshot shows the Embarcadero Cloud Platform Home dashboard. The left sidebar contains navigation links: Home, Users, Groups, Installations, EdgeModule, Resources, and Analytics. The main area displays an overview and latest statistics. At the top right, it shows "Tenant: Initial Tenant" and "CONSOLEUSER". The timestamp "Statistics at: 2019-10-21 19:57:34.844" is also present. Three cards provide key metrics: "Total Users" (1), "API calls last 24 hours" (0), and "Total Installations" (0).

| Metric                  | Value |
|-------------------------|-------|
| Total Users             | 1     |
| API calls last 24 hours | 0     |
| Total Installations     | 0     |

# Boas práticas – Padrões de utilização



# Boas práticas – Status page

facebook for developers

Documentos Ferramentas Suporte Pesquisar documentação do desenvolvedor

Painel de controle Issues Assinar Status API

 Facebook Platform is Healthy  
Desde 3 de julho às 22:13

 Past 24 hours  
Average API Response Time (ms)  
139,638 as of Há 50 minutos

 Past 24 hours  
Average API Error Rate (%)  
3,095 as of Há 50 minutos

 Past 24 hours  
Average Platform Webhook Delay Time (ms)  
714,000 as of Há 50 minutos

Histórico Últimos 90 dias

DOWNTIME PROBLEMA SAUDÁVEL

AUG SEP OCT

# Boas práticas – Status page

| North America                                                                                       | South America                      | Europe | Asia Pacific                  | Middle East | Contact Us                                                                            |
|-----------------------------------------------------------------------------------------------------|------------------------------------|--------|-------------------------------|-------------|---------------------------------------------------------------------------------------|
| <b>Recent Events</b>                                                                                |                                    |        | <b>Details</b>                |             | RSS                                                                                   |
|  No recent events. |                                    |        |                               |             |                                                                                       |
| <b>Remaining Services</b>                                                                           |                                    |        | <b>Details</b>                |             | RSS                                                                                   |
|                    | Alexa for Business (N. Virginia)   |        | Service is operating normally |             |    |
|                    | Amazon API Gateway (Montreal)      |        | Service is operating normally |             |    |
|                    | Amazon API Gateway (N. California) |        | Service is operating normally |             |    |
|                    | Amazon API Gateway (N. Virginia)   |        | Service is operating normally |             |    |
|                  | Amazon API Gateway (Ohio)          |        | Service is operating normally |             |  |
|                  | Amazon API Gateway (Oregon)        |        | Service is operating normally |             |  |
|                  | Amazon AppStream 2.0 (N. Virginia) |        | Service is operating normally |             |  |

# Boas práticas – Exemplos de códigos / SDKs

\*\* ATUALIZAÇÃO TLS

VISÃO GERAL DA API

AMBIENTE DE TESTES

INSTALAÇÃO DA API (SDK'S)

[Introdução](#)

[PHP](#)

[NodeJS](#)

[Ruby](#)

[Python](#)

[.NET](#)

[Java](#)

**Delphi**

[Go](#)

PAGAR COM BOLETO

PAGAR COM CARTÃO

## Delphi

Você está em: "[Instalação da API \(SDK's\) > Delphi](#)"

Nossa API é [RESTful](#) e responde em [JSON](#). A Gerencianet utiliza [OAuth](#) para fornecer acesso autorizado à API. Nossa SDK de Delphi já está preparada para realizar essa autenticação automaticamente.

A seguir, confira os procedimentos para instalação da SDK da Gerencianet em Delphi:

### Pré Requisitos

- Aplicações que usarão a SDK devem ser compiladas na plataforma Windows 32-bit;
- Apenas aplicações Desktop.

### Download da SDK Delphi

A SDK Delphi disponibilizada pela Gerencianet é composta de uma DLL e duas unidades que fazem a comunicação da sua aplicação com a DLL. Para fazer o download de todo o código fonte da SDK e do projeto de demonstração, [clique neste link](#). Após concluir o download, descompacte o arquivo em um diretório/pasta de sua preferência.

# Boas práticas – Fóruns de discussão

 Developers

Existing user? Sign In ▾ [Sign Up](#)

Browse Activity Leaderboard  

Forums Calendar Staff Online Users

 Home 

## Forums

PORUGUÊS 

| Topic                                                                                                                                                                                                                 | Posts       | User                                                                                               | Last Post                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| Autenticação e Autorização<br>A autenticação é a chave que fará com que você possa trabalhar com nossa API. Tire todas suas dúvidas sobre o protocolo oAuth, Access Token, Refresh token.                             | 720 posts   |  mldev          | Como fazer token não expir...<br>By mldev<br>Thursday at 07:23 PM |
| Gerenciamento de perguntas e respostas<br>O recurso de <a href="#">questions</a> e <a href="#">answers</a> permite você gerenciar toda a comunicação entre comprador e vendedor antes de ser realizada a compra.      | 125 posts   |  RETRO-GAME-NET | lista bloqueio de pergunta...<br>By RETRO-GAME-NET<br>April 28    |
| Gerenciamento de produtos<br>O recurso de <a href="#">items</a> permite controlar os anúncios do Mercado Livre. Aqui você pode tirar suas dúvidas sobre atualização de estoque, preço, categorização, variações, etc. | 2,183 posts |  LIKESOM      | Problema Atualizar Preço e...<br>By LIKESOM<br>1 hour ago         |



# Obrigado



frubim@embarcadero.com.br



fabiorubim@hotmail.com



[https://www.linkedin.com  
/in/fabiorubim/](https://www.linkedin.com/in/fabiorubim/)



<https://github.com/fabiorubim>

#37

Da sala de reunião à vida real

Embarcadero Conference 2019