



# DOCUMENTAÇÃO TÉCNICA DO SISTEMA

Versão 1.3

19/08/2025

# Índice

O que é o Power Embedded .....	4
Números do Power Embedded.....	5
Arquitetura do Power Embedded.....	6
Resumo da arquitetura .....	7
Escopo da Auditoria .....	7
Controle de Acesso.....	7
Proteção de Dados .....	7
Monitoramento e Registro de Logs.....	7
Continuidade e Recuperação .....	8
CI/CD e Versionamento.....	8
Autenticação e Controle de Acesso ao Portal.....	8
Portal de Relatórios e Autenticação .....	8
Cache e Desempenho.....	8
Comunicação com Power BI para importação dos relatórios.....	9
1. Interação com as APIs do Power BI.....	9
2. Retorno dos Metadados Necessários.....	9
3. Armazenamento dos Metadados Retornados .....	9
4. Gerenciamento pelo Administrador .....	10
5. Proteção dos Dados Pessoais .....	10
6. Não Armazenamento de Dados de Relatórios.....	10
Comunicação com Power BI para exibição dos relatórios .....	10
1. Verificação de Acesso e RLS (Row-Level Security) .....	10
2. Autenticação na API do Azure .....	11
3. Envio dos Metadados para as APIs do Power BI.....	11
4. Carregamento dos Dados e Relatórios pela API do Power BI.....	11
5. Montagem e Retorno do Iframe pelo Power BI.....	11
6. Exibição do Iframe no Power Embedded.....	12
7. Conclusão .....	12
Topologia simplificada do Power Embedded .....	13
Autenticação no portal de administração .....	13
Autenticação no portal de relatórios .....	14
Aquisição do token de acesso do Power BI para incorporar relatórios em páginas HTML.....	16

Licenciamento “Inserir para clientes” (App owns data) .....	17
Processo de Criptografia e Descriptografia de Dados Sensíveis na Aplicação .....	18
1. Introdução .....	18
2. Estrutura do Processo .....	18
2.1. Armazenamento de Dados Sensíveis .....	18
2.2. Recuperação e Descriptografia de Dados Sensíveis .....	19
2.3. Controle de Acesso ao Azure Key Vault .....	19
3. Segurança e Benefícios .....	19
4. Conclusão .....	20
Processo de Versionamento e Deploy Automatizado .....	20
1. Controle de Versionamento com Azure DevOps .....	20
2. CI/CD Automatizado .....	20
2.1. Integração Contínua (CI) .....	20
2.2. Deploy Contínuo (CD) .....	20
2.3. Aprovação e Controle .....	21
3. Segurança e Benefícios .....	21
4. Conclusão .....	21
Licenciamento do Power Embedded e da Microsoft .....	22
1. A Microsoft permite o uso do Power Embedded? .....	22
2. Posso utilizar o Power BI Pro ou Premium por Usuário para Embeddar relatórios? .....	23
3. Os usuários do Power Embedded não precisam de licença PRO? .....	25
4. Utilizar a opção de “Publicar na Web” com senha não é seguro? .....	26
5. Para acessar relatórios sem ter licença PRO não é apenas a partir do F64? .....	26
6. É possível criar, editar e publicar relatórios sem conta PRO? .....	27
7. Não posso contratar apenas o Fabric, sem o portal do Power Embedded? .....	28
Instalação do Power Embedded .....	29
Período gratuito de 30 dias do Power Embedded .....	30
Como definir a capacidade ideal para sua empresa .....	30
Como contratar uma capacidade Fabric ou Power BI Embedded .....	31
Referências .....	32

## O que é o Power Embedded

O Power Embedded é um portal web, no formato de SaaS (Software as a Service), que **utiliza uma licença por capacidade do Fabric ou Power BI Embedded para acessar as APIs oficiais do Power BI e mostrar os relatórios publicados em app.powerbi.com nesse portal 100% personalizado com a identidade visual da sua empresa.**

O acesso aos relatórios é feito via API através do licenciamento por capacidade e **o usuário que apenas visualiza os relatórios não precisará acessar o endereço app.powerbi.com, esse usuário não precisará de ter uma licença Pro do Power BI, e nem mesmo uma conta do Power BI**, pois poderá acessar o Power Embedded utilizando o email corporativo ou até mesmo, emails pessoais (Gmail, Yahoo, etc).

Como o Power Embedded utiliza o licenciamento por capacidade e não por usuário, a sua empresa não precisará mais ter dezenas/centenas de licenças Pro do Power BI, apenas para os usuários que precisam publicar relatórios ou acessar o app.powerbi.com para configuração de gateways, atualizações de dados, etc. e com isso, **o Power Embedded pode reduzir o custo de implantação e manutenção do Power BI em até 90%.**

Além da redução de custos, a solução do Power Embedded possui os seguintes benefícios:

- Inteligência artificial generativa (Power Pilot), que permite fazer perguntas para os seus dados e gerar tabelas, gráficos e análises dinamicamente, utilizando linguagem natural.
- Importação e sincronização de usuários e grupos do Entra ID, fazendo com que o sistema crie/exclua os usuários de acordo com o que acontecer com eles no grupo do Entra ID.
- Autenticação dos usuários integrada com Microsoft (Entra ID) e Google ou pelo próprio sistema, que suporta qualquer email, mesmo email pessoal (Gmail, Yahoo, Bol, etc)
- Possibilidade de compartilhar relatórios com usuários externos, sem precisar adicionar no Azure AD.
- APIs para automatizar qualquer ação administrativa e integrar com o seu sistema.
- Possibilidade de mostrar os relatórios do Power BI no seu sistema de forma transparente, sem nenhuma identidade visual do sistema e sem o usuário ter que logar novamente (Single Sign-On)
- White-label (totalmente personalizado com a identidade visual da sua empresa e de seus clientes)
- Multi-idiomas (6 idiomas suportados atualmente)
- Usuário pode editar e criar relatórios pela Web, caso tenha essa permissão ativada, sem precisar de conta Pro ou Power BI Desktop.
- Modo TV (relatórios passando automaticamente de forma nativa, sem precisar de extensão ou PC)
- Modelos dinâmicos (mesmo relatório conectado à diferentes modelos de acordo com o usuário)
- Assinatura de relatório para agendar o envio recorrente por email.

- Exportação dos dados dos visuais (CSV e Excel) e das páginas (PDF, Imagem e Power Point)
- Tudo é gerenciado por você através da área administrativa: Permissões, acessos, RLS, usuários, auditorias, e muito mais.
- Suporte a RLS, permissões via usuário ou grupo
- Diversos relatórios de auditoria, como auditoria de login, auditoria de permissão (incluindo RLS), auditoria de acesso a relatório, auditoria de capacidades, métricas de uso e várias outras.
- E muito mais!

Além de redução de custos e todas as vantagens citadas acima, saiba que todos os seus workspaces passarão a ser PREMIUM, liberando recursos no Power BI serviço que você não tem com as contas Pro:

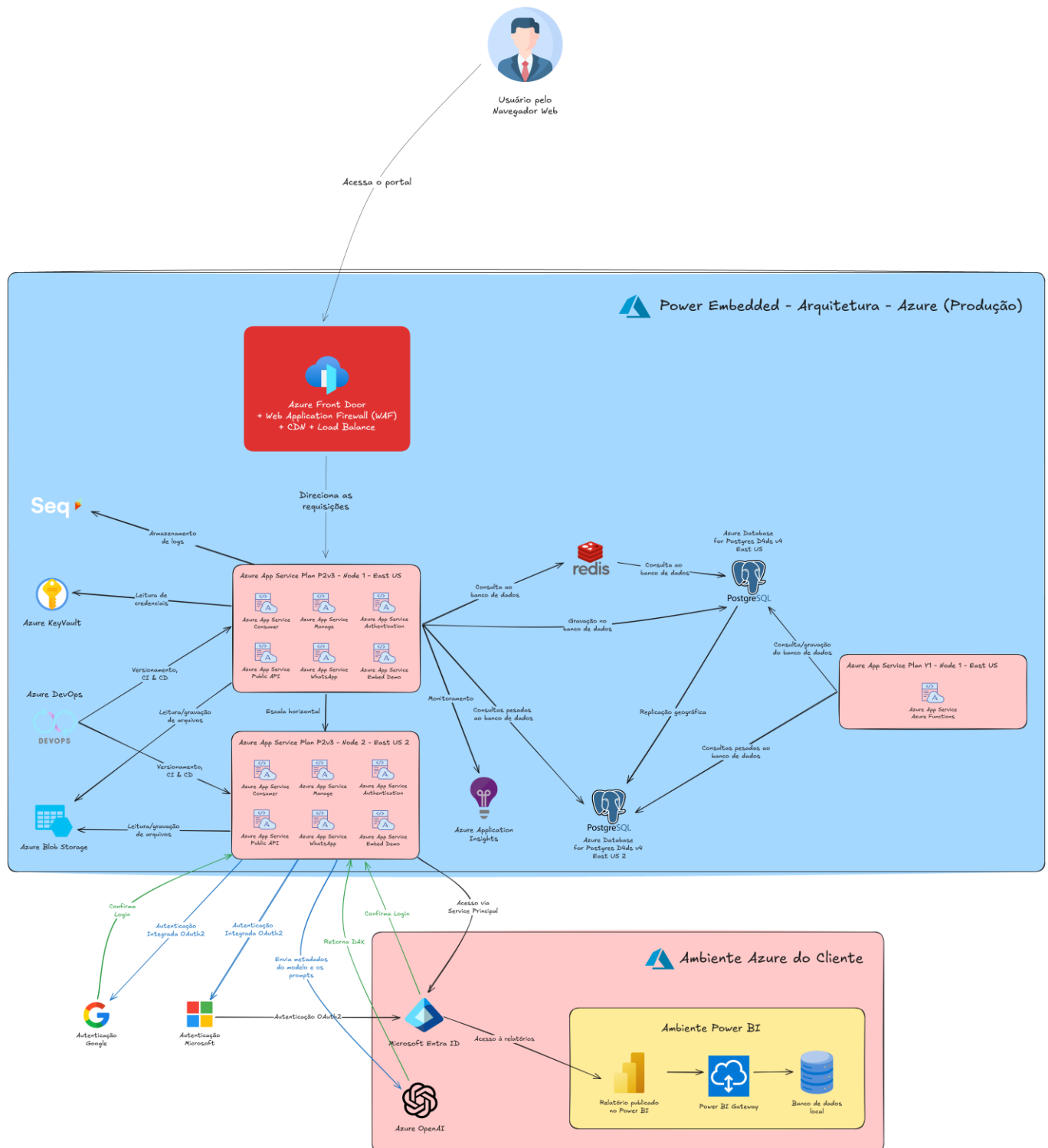
- Até 48 atualizações de dados por dia
- Conjuntos de dados maiores que 1 GB
- Datamarts (Endpoint SQL)
- Tabelas híbridas (DirectQuery + Import na mesma tabela, com dados em tempo real também)
- Versionamento nativo com GIT de relatório e modelo
- Pipelines de implantação (Criação de vários ambientes automaticamente utilizando DevOps)
- Atualização incremental de Dataflows
- Suporte para XMLA Endpoint (Permite que ferramentas externas, Como Tabular Editor, possam acessar e/ou alterar o seu modelo de dados publicado. Isso é muito utilizado para criação automática de modelos e automação de tarefas)

**Todos esses recursos estarão disponíveis após associar uma capacidade ao workspace, mesmo que você acesse o [app.powerbi.com](https://app.powerbi.com) utilizando uma conta Pro.**

## Números do Power Embedded

- 1 ano e 10 meses no mercado
- +440 empresas utilizando a plataforma
- +52.000 usuários
- +33.000 relatórios publicados
- +45.000 modelos de dados
- +255.000 regras de RLS utilizadas
- +6.200 workspaces sendo gerenciados
- +25 milhões de visualizações de relatório

# Arquitetura do Power Embedded



[https://excalidraw.com/#json=ujlxpNBfubaT990E0wbwM,bZrjEUTL9u6e1xxUo4\\_M3A](https://excalidraw.com/#json=ujlxpNBfubaT990E0wbwM,bZrjEUTL9u6e1xxUo4_M3A)

## Resumo da arquitetura

Este tópico descreve os controles internos implementados pela Power Tuning para garantir a segurança, disponibilidade e integridade dos dados na plataforma Power Embedded, hospedada no Azure App Service Premium P2V3 e utilizando Azure Database for PostgreSQL com discos Premium.

### Escopo da Auditoria

- Infraestrutura: Azure App Service Premium P2V3 (hospedagem) e Azure Database for PostgreSQL (armazenamento).
- Segurança: Controle de acesso, criptografia, monitoramento e resposta a incidentes.
- Disponibilidade: Estratégias de alta disponibilidade, failover e backup.
- Confidencialidade: Proteção de dados sensíveis e conformidade com LGPD/GDPR.
- Processos de CI/CD: Azure DevOps com controle de versionamento e rastreabilidade.

### Controle de Acesso

- Uso do Azure Active Directory (AAD), agora Microsoft Entra ID, para autenticação e autorização.
- Implementação de MFA (Multi-Factor Authentication) para acesso administrativo.
- Princípio do menor privilégio para acesso a dados e sistemas.
- Uso de RBAC (Role-Based Access Control) para gerenciar permissões e controles nos recursos de produção.

### Proteção de Dados

- Banco de dados PostgreSQL com Transparent Data Encryption (TDE) ativado.
- Uso de Azure Key Vault para gerenciamento de chaves e segredos.
- Transmissão de dados protegida com TLS 1.2+.
- Token de acesso criptografado usando RSA-OEAP, com chave armazenada no Azure Key Vault acessível apenas para líderes técnicos.
- O sistema não armazena informações sensíveis, não tem acesso aos dados dos relatórios e apenas coleta metadados, como ID do relatório, ID do workspace, ID do dataset, etc.
- As únicas informações dos usuários que são armazenadas ou tratadas no sistema são o nome (que não precisa ser nome completo) e o email corporativo.

### Monitoramento e Registro de Logs

- Logs de auditoria habilitados no Azure Database for PostgreSQL 16.8.
- Monitoramento ativo via Azure Monitor e Application Insights.
- Alertas automáticos para eventos críticos.
- Monitoramento de logins e tentativas de acesso no portal de administração.
- Implementação do Azure Defender for Cloud para proteção de dados e recursos em nuvem.

- O sistema também possui controle de logs utilizando o SEQ, a fim de centralizar logs e facilitar identificação e correção rápida de falhas.

## Continuidade e Recuperação

- Backup automático do PostgreSQL com retenção configurada.
- Plano de recuperação com testes periódicos de restore.
- Alta disponibilidade via zona de redundância do Azure.
- Servidor de aplicação e banco de dados com replicação geográfica para garantir alta disponibilidade e balanceamento de carga do ambiente.

## CI/CD e Versionamento

- Uso de Azure DevOps para Continuous Integration/Continuous Deployment (CI/CD).
- Três ambientes distintos: Desenvolvimento (Dev), Qualidade (QA) e Produção.
- Todo o código-fonte versionado no Azure DevOps, garantindo rastreabilidade e integridade.
- Cada mudança é registrada, revisada e associada a uma versão específica.
- Fluxo de CI/CD com testes automatizados para assegurar qualidade e estabilidade.
- Os processos de deploy em produção no Azure DevOps são validados e precisam ser aprovados pelo líder técnico e também pelo Product Manager, garantindo dupla validação a fim de evitar bugs e problemas em produção.

## Autenticação e Controle de Acesso ao Portal

- O portal de administração utiliza Microsoft Identity Platform para autenticação segura.
- Suporte a OAuth 2.0, OpenID Connect e Single Sign-On (SSO).
- Integração com Microsoft Entra ID para login corporativo.
- Integração com Google para autenticação externa, com suporte a 2FA.
- MFA pode ser ativado para autenticação baseada em usuário/senha.
- Possibilidade de ativar/desativar métodos de autenticação conforme necessidade da empresa.

## Portal de Relatórios e Autenticação

- O portal de relatórios permite acesso a dashboards, relatórios internos e paginados do Power BI.
- Utiliza um sistema de autenticação baseado no .NET.
- Integração com Microsoft Entra ID e Google para login externo.
- Suporte a autenticação multifator (MFA) para maior segurança.
- Controle granular sobre quais métodos de autenticação podem ser utilizados.

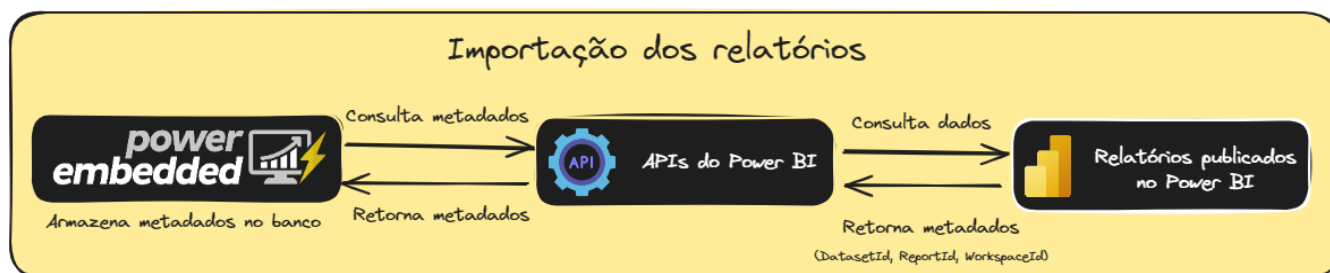
## Cache e Desempenho

- Utilização do Azure Redis para Cache para melhorar a performance e reduzir latência.



- Armazenamento temporário de informações frequentemente acessadas para otimizar as respostas do sistema.

## Comunicação com Power BI para importação dos relatórios



### 1. Interação com as APIs do Power BI

O Power Embedded utiliza as APIs oficiais do Power BI para integrar relatórios em um ambiente seguro e personalizado. A interação com as APIs é essencial para a coleta de metadados necessários para a exibição dos relatórios no portal.

- **Autenticação e autorização:** O Power Embedded se conecta às APIs do Power BI usando autenticação segura, garantindo que apenas usuários autorizados possam acessar os relatórios.
- **Coleta de metadados:** Durante a conexão, o Power Embedded requisita informações como IDs de Workspaces, Relatórios e Conjuntos de Dados, que são fundamentais para o funcionamento do portal.

### 2. Retorno dos Metadados Necessários

Após a interação inicial, as APIs do Power BI retornam os metadados essenciais para a configuração dos relatórios no portal.

- **IDs de Workspaces, Relatórios e Conjuntos de Dados:** Esses identificadores permitem ao Power Embedded exibir corretamente os relatórios de acordo com as permissões do usuário.
- **Segurança dos dados:** Somente metadados são retornados; nenhum dado de conteúdo dos relatórios é armazenado ou trafega pelos servidores do Power Embedded.

### 3. Armazenamento dos Metadados Retornados

Os metadados coletados das APIs do Power BI são armazenados no Power Embedded para gerenciar a exibição dos relatórios.

- **Armazenamento seguro:** Os metadados são armazenados de maneira segura, sem comprometimento de informações sensíveis.
- **Uso exclusivo para exibição:** Os metadados são utilizados exclusivamente para exibição e gerenciamento dos relatórios no portal, sem armazenamento de dados pessoais dos usuários além do essencial.

## 4. Gerenciamento pelo Administrador

O administrador do Power Embedded possui controle total sobre as configurações de exibição dos relatórios, garantindo uma experiência segura e personalizada para os usuários.

- **Permissões e RLS (Row-Level Security):** O administrador define as permissões de acesso e configurações de RLS para assegurar que cada usuário veja apenas os dados aos quais tem direito.
- **Estrutura de pastas e organização:** O portal permite ao administrador criar uma estrutura organizada de pastas para fácil navegação e acesso aos relatórios.
- **Configuração de atributos de relatórios:** O administrador pode ajustar atributos específicos dos relatórios, como visibilidade e configurações de compartilhamento.

## 5. Proteção dos Dados Pessoais

O Power Embedded adota políticas rigorosas de privacidade e proteção de dados, garantindo que nenhum dado pessoal sensível seja armazenado.

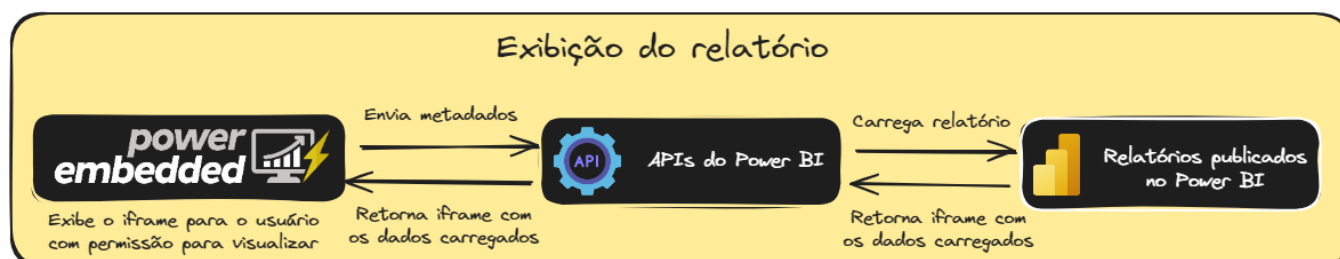
- **Armazenamento mínimo de dados pessoais:** Somente o email e o nome dos usuários são armazenados, necessários para autenticação e atribuição de permissões.
- **Conformidade com regulamentações:** A solução segue as melhores práticas de conformidade com regulamentações de privacidade, como GDPR e LGPD.

## 6. Não Armazenamento de Dados de Relatórios

O Power Embedded não armazena, processa ou transmite dados de relatórios, garantindo a segurança e privacidade das informações.

- **Tráfego seguro direto ao Power BI:** Toda a exibição dos relatórios é realizada diretamente a partir das APIs do Power BI, sem passagem de dados pelo Power Embedded.
- **Zero retenção de dados de relatórios:** Nenhum dado de relatório é armazenado ou trafega pelos servidores do Power Embedded, assegurando a integridade e segurança das informações.

## Comunicação com Power BI para exibição dos relatórios



### 1. Verificação de Acesso e RLS (Row-Level Security)

Quando um usuário tenta acessar um relatório, o Power Embedded primeiro verifica se o usuário logado tem permissão para visualizar o conteúdo.

- **Verificação de permissões:** Com base nas configurações definidas pelo administrador, o sistema verifica se o usuário tem acesso ao relatório específico.
- **Envio de dados para RLS:** Caso o relatório utilize Row-Level Security (RLS), o Power Embedded envia as informações de acesso do usuário (email) e nome da função de segurança associada ao usuário, para aplicar as restrições definidas.
- **Garantia de segurança:** Nenhum dado sensível do relatório é acessado durante esse processo; apenas informações de controle de acesso são utilizadas.

## 2. Autenticação na API do Azure

Para garantir a segurança e a conformidade com as melhores práticas, o Power Embedded se autentica na API do Azure antes de interagir com as APIs do Power BI.

- **Autenticação segura:** O Power Embedded utiliza métodos de autenticação segura para se conectar à API do Azure, garantindo que apenas usuários e sistemas autorizados tenham acesso.
- **Recuperação de token:** Durante a autenticação, o Power Embedded obtém um token que será usado para autenticar todas as requisições subsequentes às APIs do Power BI.

## 3. Envio dos Metadados para as APIs do Power BI

Após a autenticação, o Power Embedded envia os metadados necessários para a exibição do relatório.

- **Envio de IDs:** O sistema envia os IDs do Workspace, Relatório e Conjunto de Dados para as APIs do Power BI. Esses metadados são essenciais para que o Power BI localize e carregue o relatório correto.
- **Segurança dos metadados:** Apenas os metadados são enviados, sem que dados do conteúdo dos relatórios sejam compartilhados ou armazenados pelo Power Embedded.

## 4. Carregamento dos Dados e Relatórios pela API do Power BI

A API do Power BI utiliza os metadados fornecidos pelo Power Embedded para carregar os dados e montar o relatório.

- **Carregamento direto dos workspaces:** Os dados armazenados nos workspaces são carregados pela API do Power BI, sem passar pelos servidores do Power Embedded.
- **Processamento seguro:** O processamento dos dados e a montagem do relatório ocorrem inteiramente nos servidores do Power BI, garantindo que os dados permaneçam seguros.

## 5. Montagem e Retorno do Iframe pelo Power BI

Após o carregamento dos dados, a API do Power BI monta o elemento iframe que aponta para o relatório já pronto.

- **Criação do iframe:** A API do Power BI cria o iframe que contém o relatório e ajusta as configurações de exibição, como filtros aplicados e RLS.
- **Retorno para o Power Embedded:** O iframe é então retornado ao Power Embedded para exibição ao usuário final.

## 6. Exibição do Iframe no Power Embedded

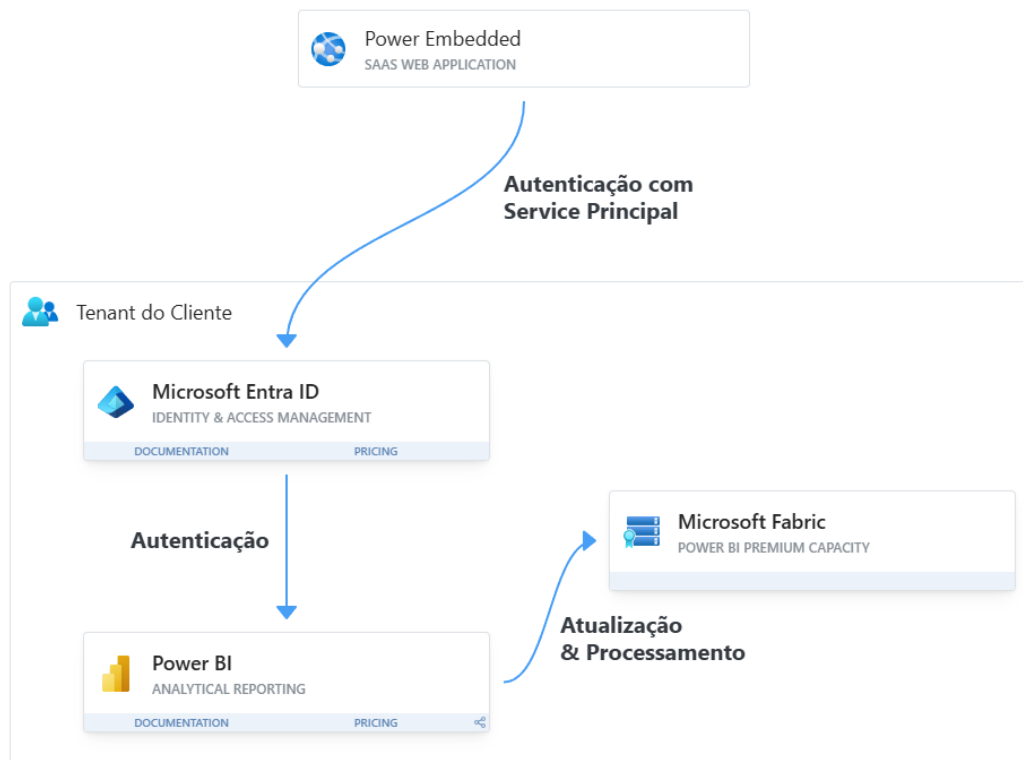
O Power Embedded exibe o iframe retornado diretamente para o usuário, sem acessar, ler ou armazenar nenhum dado do relatório.

- **Exibição segura:** O iframe é embutido no portal, e o usuário visualiza o relatório como se estivesse acessando diretamente pelo Power BI.
- **Zero tráfego de dados:** Nenhum dado do relatório trafega pelos servidores do Power Embedded, assegurando que as informações permaneçam inteiramente no ambiente seguro do Power BI.
- **Garantia de privacidade:** A solução segue rigorosamente as diretrizes de privacidade, com nenhum dado de relatório sendo processado ou retido pelo sistema.

## 7. Conclusão

O Power Embedded oferece uma solução robusta e segura para a exibição de relatórios do Power BI, integrando autenticação avançada e verificações de acesso para garantir que os dados permaneçam protegidos. Todo o processamento dos relatórios ocorre diretamente nos servidores do Power BI, assegurando que as informações dos relatórios sejam exibidas aos usuários de forma segura e conforme as permissões definidas.

## Topologia simplificada do Power Embedded



## Autenticação no portal de administração

O portal de administração é responsável por configurar e gerenciar todo o ambiente do cliente dentro do Power BI. É nele que administradores têm controle sobre permissões, segurança, governança e outras definições importantes para garantir o funcionamento adequado dos recursos.

Os itens do Power BI Service gerenciados no portal de administração são apenas metadados, ou seja, informações como quem tem acesso, relatórios disponíveis e políticas aplicadas.

É importante destacar que o portal de administração não possui acesso aos dados em si, mantendo a segurança e privacidade das informações dos usuários e das organizações.

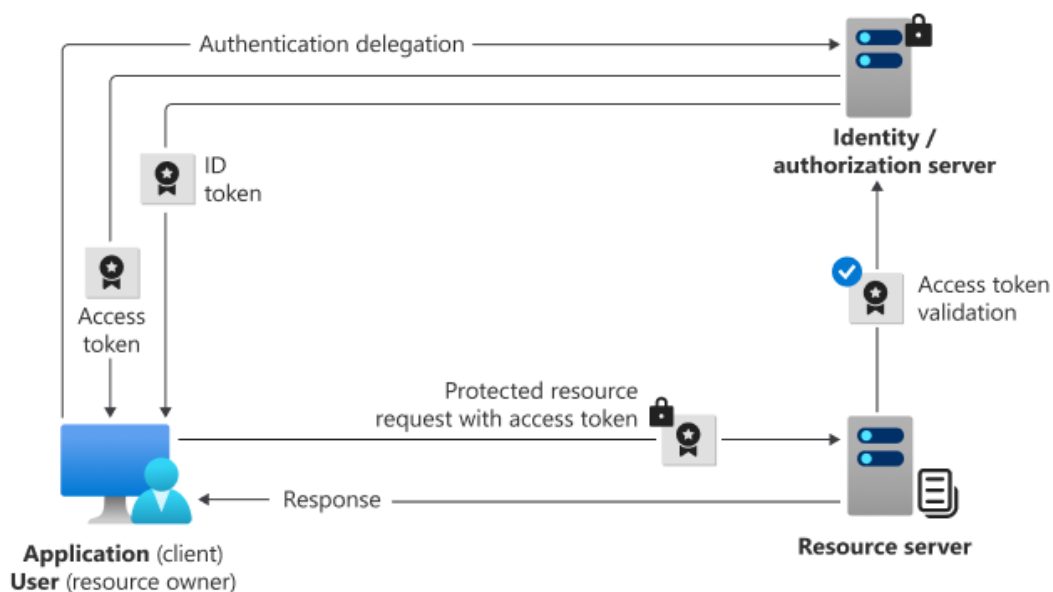
A autenticação no portal de administração utiliza a Microsoft Identity Platform, uma solução integrada que fornece autenticação robusta e segura baseada em padrões como OAuth 2.0 e OpenID Connect.

A Microsoft Identity Platform facilita a autenticação de usuários e a autorização de acesso, oferecendo suporte para Single Sign-On (SSO) e integração com diferentes tipos de identidades, como contas corporativas (Azure AD) e pessoais (Microsoft Accounts).

Toda a configuração de autenticação e segurança é feita e controlada pelo cliente, dentro do ambiente de sua tenant, via Entra ID (anteriormente conhecido como Azure AD).

Isso permite que o cliente aproveite todo o poder da Azure para garantir a proteção do portal de administração, incluindo políticas de segurança, autenticação multifator (MFA) e controle de acesso condicional.

Essa flexibilidade garante que o cliente tenha total controle sobre quem acessa seu ambiente e como esse acesso é protegido.



#### Observações:

- O usuário (proprietário do recurso) inicia uma solicitação de autenticação com o provedor de identidade/servidor de autorização a partir da aplicação cliente;
- Se as credenciais forem válidas, o provedor de identidade/servidor de autorização envia primeiro um token de ID contendo informações sobre o usuário para a aplicação cliente;
- O provedor de identidade/servidor de autorização obtém o consentimento do usuário final e concede autorização à aplicação cliente para acessar o recurso protegido.
- A autorização é fornecida em um token de acesso, que também é enviado para a aplicação cliente;
- O token de acesso é anexado às solicitações subsequentes feitas ao servidor de recursos protegidos pela aplicação cliente;
- O provedor de identidade/servidor de autorização valida o token de acesso;
- Se a validação for bem-sucedida, a solicitação pelos recursos protegidos é concedida, e uma resposta é enviada para a aplicação cliente.

Para mais informações sobre o Microsoft identity Platform, acesse o link abaixo:

<https://learn.microsoft.com/en-us/entra/identity-platform/>

## Autenticação no portal de relatórios

O portal de relatórios é o local onde os usuários têm acesso a diversos tipos de conteúdos, como relatórios internos e externos, relatórios paginados, dashboards e outros recursos gerados no Power BI. É por meio desse portal que eles podem consumir e interagir com as informações de maneira prática e centralizada.

Ele utiliza um sistema de autenticação gerenciado pelo **.NET**, que aborda todos os principais desafios de gerenciamento de identidade, como login, recuperação de senha, troca de senha e outras funcionalidades essenciais.

Esse sistema de identidade está no mercado há muitos anos e é amplamente reconhecido como um dos mais seguros e confiáveis do mundo, sendo adotado por organizações globais para garantir a proteção dos dados de seus usuários.

O portal de relatórios pode ser integrado com o **Microsoft Entra ID** (anteriormente Azure AD) para autenticação externa. Essa integração permite que os usuários façam login utilizando suas credenciais corporativas, o que oferece uma experiência de autenticação única (Single Sign-On) e o poder de utilizar todas as ferramentas de segurança da Azure, como autenticação multifator (MFA), controle de acesso condicional e políticas de

segurança robustas. Com o Entra ID, as empresas podem gerenciar acessos com base em grupos, permissões e outras políticas definidas na tenant do cliente.

Além do Entra ID, o portal de relatórios também oferece integração com o Google para autenticação externa. Isso permite que usuários que possuem contas no Google utilizem suas credenciais para acessar o portal de relatórios, facilitando a integração com ambientes de trabalho que utilizam o ecossistema Google, como o Google Workspace.

Essa integração também pode ser configurada com medidas adicionais de segurança, como o uso de autenticação de dois fatores (2FA), oferecida pelo Google.

Para garantir maior personalização e segurança, os tipos de autenticação disponíveis (usuário/senha, Microsoft ou Google) podem ser ativados/desativados conforme as necessidades do cliente. Isso significa que os usuários só poderão se autenticar utilizando os métodos permitidos pela empresa.

Por exemplo, se a organização habilitar somente a autenticação via Entra ID, os usuários serão obrigados a usar suas credenciais Microsoft para acessar o portal e não conseguirão acessar o portal utilizando autenticação Google ou email/senha.

Além disso, para o tipo de autenticação baseado em usuário e senha, pode ser configurada a autenticação multifator (MFA) para adicionar uma camada extra de segurança.

Com o MFA habilitado, os usuários precisam fornecer uma segunda forma de verificação, como um código enviado para o e-mail do usuário, para acessar o portal.

O portal de administração oferece uma visão completa sobre os logins realizados no portal de relatórios. Ele permite que os administradores monitorem todos os acessos, mostrando a status das tentativas de login (se foram bem-sucedidas ou falhas), data da tentativa e qual método de autenticação foi utilizado e qual usuário tentou realizar o login.

Isso garante que a segurança do ambiente seja auditável e controlada, proporcionando transparência sobre o comportamento de acesso dos usuários.

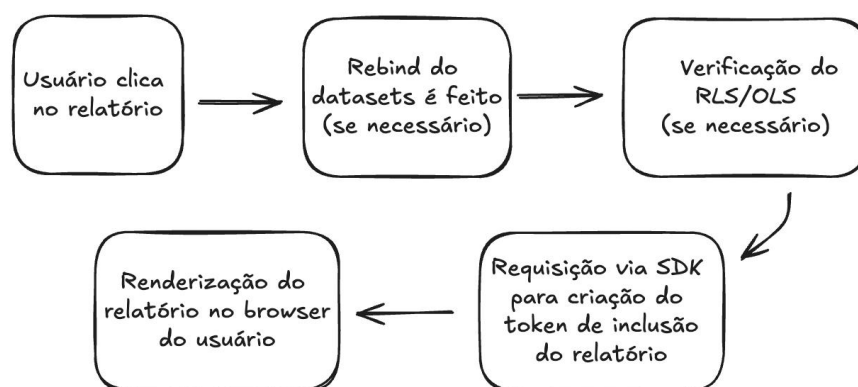
## Aquisição do token de acesso do Power BI para incorporar relatórios em páginas HTML

Com o Power Embedded, tokens de incorporação são gerados em tempo real, permitindo que os usuários acessem relatórios, dashboards e visuais do Power BI diretamente no portal de relatórios, sem a necessidade de possuir uma licença do Power BI.

Isso proporciona uma experiência de integração transparente, onde os usuários podem visualizar e interagir com os dados de maneira intuitiva, sem interrupções ou exigências adicionais de permissões.

Essa solução é ideal para organizações que desejam compartilhar insights e relatórios com seus usuários finais dentro de suas próprias aplicações ou portais, mantendo a personalização e o controle de acesso, sem que os usuários precisem adquirir licenças individuais do Power BI.

O uso dos tokens garante a segurança e a flexibilidade no controle dos acessos, enquanto mantém a eficiência no compartilhamento de informações.



Durante o processo de geração do token de incorporação do Power Embedded, as etapas envolvidas são as seguintes:

1. **Seleção do item a ser renderizado:** O primeiro passo é selecionar o relatório, dashboard ou visual do Power BI que será incorporado no portal de relatórios. Este item será preparado para ser exibido ao usuário final.;
2. **Rebind (caso seja necessário):** Se for necessário reapontar o dataset de um relatório para outro, ocorre o processo de Rebind. Esse recurso permite redirecionar o relatório para um dataset diferente, desde que ambos tenham a mesma estrutura de dados. Isso é crucial para garantir o isolamento completo dos dados entre clientes e usuários, possibilitando que cada cliente acesse seus próprios dados sem interferência, mesmo usando o mesmo relatório.;
3. **RLS/OLS (Row-Level Security - Object-Level Security):** Caso seja necessário, a Segurança a nível de Linha (ou Segurança a nível de Object) é aplicada. Essa funcionalidade permite a implementação de filtros automáticos nos dados, com base no usuário logado. Dessa forma, o usuário só terá acesso às informações às quais tem permissão, garantindo que os dados exibidos no relatório sejam personalizados conforme as regras de segurança definidas no modelo de dados.;
4. **Requisição via SDK para aquisição do token de acesso para o usuário:** através da SDK do Power BI, é realizada uma requisição para gerar o token de incorporação. Esse token autoriza o usuário a visualizar o relatório ou dashboard no portal de relatórios, garantindo que a autenticação e as permissões estejam corretas.;



5. **Renderização do relatório no navegador do usuário:** após a geração e validação do token, o relatório é renderizado diretamente no navegador do usuário. Todo o processo é transparente e o conteúdo é exibido de forma interativa, permitindo ao usuário final acessar os insights do Power BI sem a necessidade de uma licença individual, mas com total controle de segurança e isolamento de dados.

## Licenciamento “Inserir para clientes” (App owns data)

Cada **cliente tem:**

- Seu **próprio tenant Microsoft Entra ID**
- Suas **capacidades Premium (Power BI Embedded ou Fabric)**
- Seus próprios **workspaces com relatórios, associados com 1 capacidade Premium**
- Um **service principal criado no tenant dele**, concedendo permissão somente aos workspaces usados no portal.

O Power Embedded (no tenant da ISV):

- Autentica usando o **client\_id + secret do service principal do cliente**
- Gera o **token de embed** com escopo mínimo
- Aplica segurança e RLS com base no banco de dados interno da ISV
- Não possui controle ou hospedagem dos relatórios, apenas os consome via API

Pontos importantes:

- Os **usuários são do próprio tenant deles** ou usuários externos, cadastrados por um administrador do portal via SSO ou métodos alternativos (Entra ID, Google, Email/senha, etc.).
- O **acesso aos relatórios é feito via autenticação não interativa**, conforme definido pela Microsoft para ISVs no modelo "inserir para seus clientes".
- A Power Tuning, como ISV, cria um **Service Principal diretamente dentro do tenant do cliente** (com consentimento deles), e o configura com as permissões adequadas para gerar o token de embed.
- O Power Embedded **atua como um middleware**, mas o acesso e o embed ocorrem usando o **Service Principal daquele tenant**, com capacidade vinculada àquele tenant.
- Mesmo que o portal seja multicliente, **cada tenant tem sua própria instância de embed isolada**, com seu próprio Service Principal e sua própria capacidade.
- Os usuários finais **não precisam de licenças Power BI Pro**, desde que os relatórios estejam atribuídos a uma capacidade dedicada.
- Como o conteúdo e o Service Principal estão no **mesmo tenant do cliente**, não há violação do controle de dados nem do isolamento entre tenants.

# Processo de Criptografia e Descriptografia de Dados Sensíveis na Aplicação

O Power Embedded prioriza a segurança dos dados armazenados em sua base de dados. Para isso, adota as melhores práticas de desenvolvimento e armazenamento de dados, além de seguir rigorosamente as normas de compliance recomendadas tanto pela comunidade quanto pela Microsoft.

Essas boas práticas garantem a integridade, privacidade e proteção dos dados, proporcionando uma solução confiável e alinhada com os padrões globais de segurança da informação.

Os dados dos clientes são organizados para serem separados logicamente dentro da base de dados e da aplicação, assegurando que um cliente não tenha acesso a ler ou modificar as informações de outros clientes.

Essa segregação lógica protege a privacidade dos dados e impede qualquer forma de acesso indevido entre diferentes usuários.

Este tópico descreve o processo de armazenamento, recuperação e proteção de dados sensíveis, como secrets de Service Principal e chaves de API, utilizando criptografia RSA-OAEP em uma aplicação integrada com o Azure Key Vault.

## 1. Introdução

Para garantir a segurança dos dados sensíveis, a aplicação armazena informações confidenciais de forma criptografada no banco de dados. A criptografia é realizada utilizando o algoritmo RSA-OAEP, proporcionando uma camada adicional de segurança contra acesso não autorizado.

## 2. Estrutura do Processo

### 2.1. Armazenamento de Dados Sensíveis

1. **Entrada de Dados:** A aplicação coleta dados sensíveis, como secrets do Service Principal e chaves de API, que precisam ser protegidos contra acessos não autorizados.
2. **Criptografia com RSA-OAEP:**
  - Os dados sensíveis são criptografados utilizando o algoritmo RSA-OAEP.
  - Um par de chaves RSA (pública e privada) é utilizado para esse processo:
    - **Chave Pública:** Usada para criptografar os dados antes de serem armazenados.
    - **Chave Privada:** Mantida segura no Azure Key Vault e utilizada apenas para a descriptografia dos dados.
3. **Armazenamento no Banco de Dados:**
  - Os dados criptografados são armazenados no banco de dados da aplicação, garantindo que, mesmo que o banco seja comprometido, os dados sensíveis permaneçam protegidos.

## 2.2. Recuperação e Descriptografia de Dados Sensíveis

### 1. Necessidade de Descriptografar os Dados:

- Quando a aplicação precisa acessar os dados sensíveis para realizar alguma operação, é necessário descriptografá-los.

### 2. Recuperação da Chave de Descriptografia:

- A aplicação precisa da chave privada para descriptografar os dados.
- A chave privada nunca é armazenada na aplicação ou no banco de dados. Em vez disso, ela é mantida de forma segura no **Azure Key Vault**.

### 3. Azure Key Vault e Chaves de Cliente:

- Cada cliente da aplicação possui sua própria chave de descriptografia, armazenada no Azure Key Vault.
- As chaves são geradas de forma aleatória e automática durante a instalação da aplicação quando o administrador clica no botão "Criar organização".

### 4. Processo de Descriptografia:

- A aplicação se autentica no Azure Key Vault e solicita a chave de descriptografia associada ao cliente específico.
- O Azure Key Vault retorna a chave de descriptografia de forma segura.
- A aplicação usa a chave para descriptografar os dados sensíveis e prosseguir com a operação desejada.

## 2.3. Controle de Acesso ao Azure Key Vault

- **Acesso Restrito:** O acesso ao Azure Key Vault é rigorosamente controlado e limitado a apenas dois papéis críticos:
  - **Arquiteto Principal da Aplicação:** Responsável pela segurança e configuração do Key Vault.
  - **Gerente do Produto:** Responsável pela aprovação de acessos e controle de segurança.
- **Restrição ao Time de Desenvolvimento:** Nenhum outro funcionário, incluindo o time de desenvolvimento, tem acesso às chaves de descriptografia, garantindo que essas chaves permaneçam altamente protegidas e minimizando riscos de exposição.

## 3. Segurança e Benefícios

- **Segregação de Dados:** Cada cliente possui sua própria chave de descriptografia, garantindo que os dados sejam isolados e acessíveis apenas pela chave correta.
- **Controle Rigoroso de Acesso:** Com acesso restrito ao Azure Key Vault, a segurança das chaves de descriptografia é garantida, tornando extremamente difícil o acesso não autorizado.

## 4. Conclusão

O processo descrito assegura que os dados sensíveis da aplicação sejam armazenados e recuperados de forma segura, utilizando o Azure Key Vault para proteger as chaves decriptografia, protegendo as informações confidenciais dos clientes.

# Processo de Versionamento e Deploy Automatizado

## 1. Controle de Versionamento com Azure DevOps

### Versionamento de Código:

- Todo o código-fonte da aplicação é controlado por versionamento no Azure DevOps, garantindo rastreabilidade e integridade das alterações.
- Cada mudança é registrada, revisada e associada a uma versão específica, permitindo que as implementações sejam gerenciadas de forma organizada.

## 2. CI/CD Automatizado

O processo de CI/CD (Continuous Integration/Continuous Deployment) é utilizado para garantir que as mudanças na aplicação sejam integradas, testadas e implantadas de maneira eficiente e segura. O fluxo é dividido em etapas para assegurar a qualidade do código e a estabilidade da aplicação em produção.

### 2.1. Integração Contínua (CI)

- **Objetivo:** Integrar as mudanças de código frequentemente, testando e validando cada modificação para evitar conflitos e garantir a qualidade do software.
- **Etapas do CI:**
  1. **Commit e Pull Requests:** Desenvolvedores enviam as mudanças de código para o repositório.
  2. **Compilação Automática:** O pipeline CI é acionado, e o código é compilado automaticamente para garantir que não haja erros de build.
  3. **Testes Automatizados:** Execução de testes unitários, de integração e de segurança para validar o funcionamento correto das alterações.
  4. **Relatório de Resultados:** O pipeline gera relatórios detalhados com os resultados dos testes, identificando falhas que precisam ser corrigidas.

### 2.2. Deploy Contínuo (CD)

- **Objetivo:** Automatizar a implantação das mudanças validadas em múltiplos ambientes, assegurando que cada etapa seja rigorosamente testada antes de chegar à produção.

- **Ambientes de Implantação:**

1. **Desenvolvimento:**

- Utilizado para testes iniciais de novas funcionalidades.
- Alterações são implantadas automaticamente para identificar e corrigir problemas rapidamente.

2. **Homologação:**

- Simula o ambiente de produção e é usado para validação completa de todas as funcionalidades.
- Executa testes de integração completos, testes de carga e verificações de conformidade.

3. **Produção:**

- Apenas as mudanças aprovadas pelo gerente de produtos são implantadas neste ambiente.
- As alterações passam por um processo de aprovação manual para garantir que todas as validações anteriores foram cumpridas.

## 2.3. Aprovação e Controle

- **Aprovação pelo Gerente de Produtos:**

- Antes de qualquer mudança ser implantada em produção, ela deve ser aprovada pelo gerente de produtos.
- Isso garante que as alterações atendem aos requisitos de negócio e que o código passou por todas as etapas de validação.

## 3. Segurança e Benefícios

- **Versionamento e Validação de Código:** O uso de Azure DevOps e pipelines de CI/CD garante que todas as mudanças sejam controladas e validadas antes de chegarem ao ambiente de produção, reduzindo significativamente o risco de falhas.
- **Automação e Eficiência:** A automação do processo de deploy minimiza erros manuais e acelera o ciclo de desenvolvimento, mantendo a aplicação atualizada e segura.

## 4. Conclusão

O processo descrito assegura que as mudanças no código passem por um rigoroso processo de validação e aprovação. Com controle de acesso restrito e automação de deploy, a aplicação se mantém alinhada com as melhores práticas de segurança e governança, mantendo a estabilidade da plataforma.

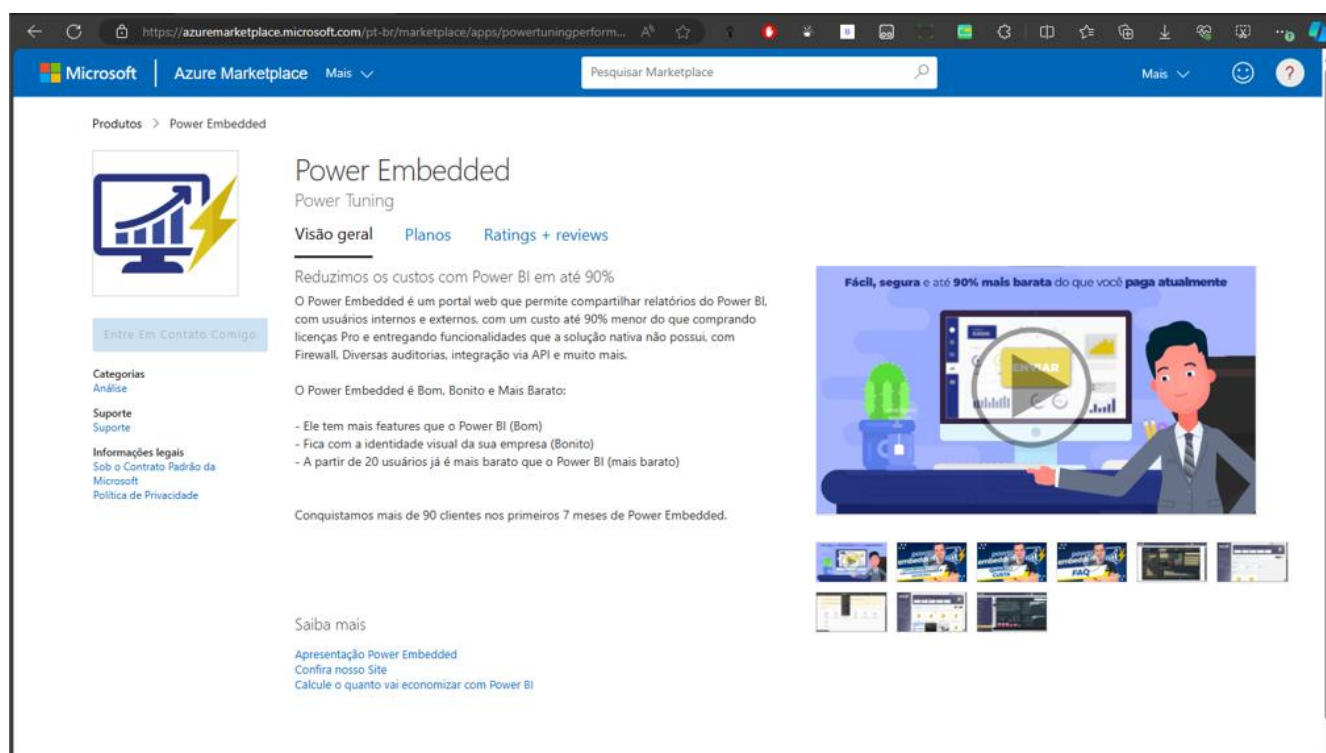
# Licenciamento do Power Embedded e da Microsoft

## 1. A Microsoft permite o uso do Power Embedded?

Uma pergunta bem comum de vários clientes é em relação ao licenciamento do Power Embedded.

Com certeza, a Microsoft permite o uso do Power Embedded e é uma solução 100% legal. A Power Tuning é uma empresa Microsoft Solutions Partner desde 2018, e uma das líderes em vendas de Azure no Brasil e, portanto, tem um forte relacionamento com a Microsoft e a distribuidora TD Synnex, e em hipótese alguma iria desenvolver um produto que utilizasse alguma licença ilegal ou mecanismo que quebre o contrato de uso com a Microsoft.

O Power Embedded também está disponível para ser acessado e contratado pelo [Azure Marketplace](https://azuremarketplace.microsoft.com/pt-br/marketplace/apps/powerembeddingperform...), o que indica um forte relacionamento com a Microsoft para suportar o produto.



## 2. Posso utilizar o Power BI Pro ou Premium por Usuário para Embeddar relatórios?

Uma pergunta bem comum feita por quem não conhece muito bem do licenciamento do Power BI, é se é possível utilizar o Power BI Pro ou Premium por Usuário para Embeddar os relatórios em portais Web.

A resposta é sim, é possível gerar tokens para Embeddar relatórios em uma capacidade Pro ou Premium por Usuário, mas de acordo com a [documentação oficial da Microsoft](#):

### Testes de desenvolvimento

Para testes de desenvolvimento, você pode usar tokens de avaliação de inserção gratuitos com uma licença Pro ou PPU (Premium por usuário). Para fazer uma inserção em um ambiente de produção, use uma capacidade.

#### ⓘ Importante

Os tokens de avaliação gratuitos são limitados apenas a testes de desenvolvimento. Depois de ir para a produção, deve ser adquirida uma capacidade. Até que uma capacidade seja adquirida, a faixa de *versão de avaliação gratuita* continuará a aparecer na parte superior do relatório inserido.

O número de tokens de avaliação de inserção que uma *entidade de serviço* ou um *usuário mestre* (conta mestra) do Power BI pode gerar é limitado. Use a API [Recursos disponíveis](#) para verificar o percentual de seu uso inserido atual. O valor de uso é exibida por entidade de serviço ou conta mestra.

Se você ficar sem tokens de inserção durante o teste, precisará comprar uma capacidade do Power BI Embedded ou Premium. Não há limite quanto à quantidade de tokens inseridos que você pode gerar com uma capacidade.

Ou seja, você pode sim, utilizar relatórios que estejam em um workspace utilizando uma capacidade Pro ou Premium por Usuário (PPU) para desenvolver ou testar alguma solução de Embedded, pois a Microsoft disponibiliza uma quantidade LIMITADA de tokens para serem utilizados para embeddar relatórios externamente, mas quando essa quantidade de tokens acabar, você não irá conseguir mais utilizar essa conta PRO para isso, os processos existentes vão parar de funcionar e você precisará **contratar uma capacidade dedicada para continuar utilizando**.

Por este motivo, não recomendamos, em nenhuma hipótese, nem cogitar implantar um processo desses em produção sem utilizar uma capacidade dedicada (Fabric ou Power BI Embedded).

**Observação:** Neste artigo estamos considerando o cenário de utilizar as APIs do Power BI para mostrar relatórios do Power BI em aplicações e portais Web. Os recursos do menu Inserir relatório (Publicar na Web, Sharepoint Online e Site/portal) não utilizam a API do Power BI para geração de tokens e autenticação, e por isso, podem ser utilizadas utilizando conta PRO/PPU normalmente.

A página de [perguntas e respostas do Power BI Embedded](#) reafirma que contas Pro não podem ser utilizadas para soluções de Embedded em produção:

*“Os tokens inseridos com a licença Pro ou PPU (Premium por usuário) destinam-se para teste de desenvolvimento, portanto, uma conta mestre ou [entidade de serviço](#) do Power BI pode gerar apenas um número limitado de tokens. [Compre uma capacidade](#) para inserir em um ambiente de produção. Não há limites para a quantidade de tokens inseridos que você pode gerar ao comprar uma capacidade. Em*



testes de desenvolvimento, você pode usar tokens de avaliação de inserção gratuitos com uma licença Pro. Para fazer uma inserção em um ambiente de produção, você deve comprar uma capacidade.”

A página [Cenários de uso do Power BI: inserir para clientes – Power BI | Microsoft Learn](#) também reforça que o uso de uma capacidade é obrigatório para utilizar tecnologias de Embedded:

## Licenciamento

Ao inserir conteúdo do Power BI para clientes, você precisa garantir que o conteúdo resida em um workspace que tenha um dos seguintes modos de licença:

- Capacidade Premium: esse modo de licença está disponível com o [Power BI Premium](#).
- Embedded – esse modo de licença está disponível com o [Power BI Embedded](#) <sup>↗</sup>.
- Capacidade do Fabric: esse modo de licença está disponível com o [Microsoft Fabric](#).

### 📘 Importante

Às vezes, este artigo se refere ao Power BI Premium ou às suas assinaturas de capacidade (P SKUs). Lembre-se de que a Microsoft está consolidando atualmente as opções de compra e desativando os SKUs do Power BI Premium por capacidade. Em vez disso, os clientes novos e existentes devem considerar a compra de SKUs (assinaturas de capacidade do Fabric).

Para obter mais informações, confira [Atualização importante para o licenciamento do Power BI Premium](#) <sup>↗</sup> e [Perguntas frequentes do Power BI Premium](#).

Cada opção de modo de licença requer a compra de um produto faturável que seja uma licença baseada em capacidade. Uma licença baseada em capacidade permite que você crie capacidades reservadas.

As capacidades representam os recursos computacionais necessários para processar cargas de trabalho, como renderização de relatório e atualização de dados. As capacidades reservadas são isoladas das cargas de trabalho de outros clientes, portanto, oferecem escala que pode fornecer desempenho confiável e consistente.

### 📘 Observação

Não é possível usar o cenário de *Inserção para os seus clientes* em ambientes de produção com as licenças do Fabric (gratuita), Power BI Pro ou Power BI PPU.

Para obter mais informações sobre produtos e licenciamento, consulte [Selecionar o produto apropriado de análise integrada do Power BI](#).



Além disso, essa mesma página informa que o conteúdo que será mostrado na aplicação NÃO PODE estar em um workspace pessoal:

## Conteúdo inserível

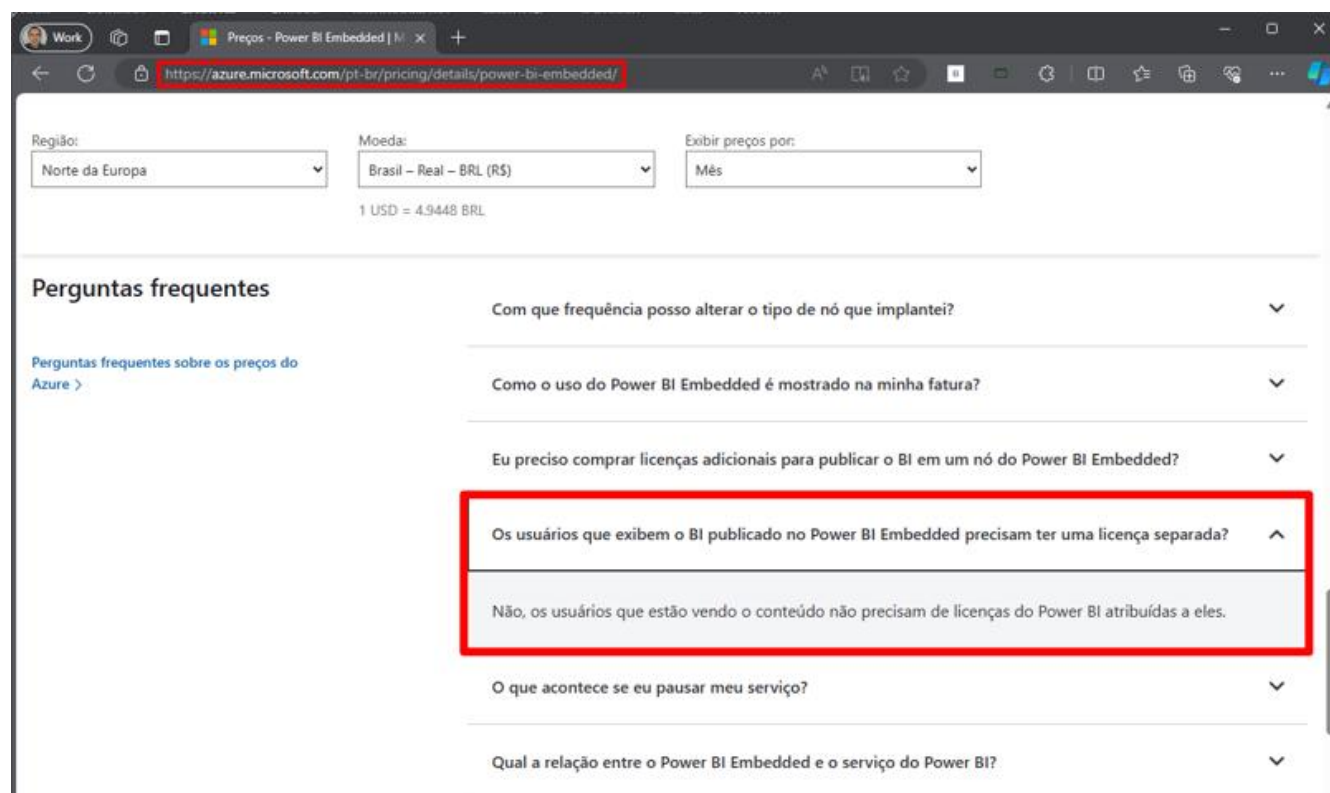
Você pode inserir os seguintes tipos de conteúdo do Power BI para os clientes:

- Relatórios do Power BI
- Visuais de relatórios específicos do Power BI
- Relatórios paginados
- Experiência de P e R
- Painéis
- Blocos de dashboard específicos

Não há nenhuma limitação sobre onde o conteúdo reside, exceto pelo fato de que o conteúdo não pode residir em um workspace pessoal. O que importa é que a identidade de inserção tenha permissão para exibir (ou criar ou editar) o conteúdo.

## 3. Os usuários do Power Embedded não precisam de licença PRO?

Falando sobre o licenciamento por capacidade, no [link abaixo](https://azure.microsoft.com/pt-br/pricing/details/power-bi-embedded/), a Microsoft deixa bem claro que os usuários que estão vendo o conteúdo publicado no Power BI Embedded não precisam de licenças do Power BI atribuídas a eles, portanto, não é necessário uma licença PRO para visualização dos relatórios através do Power Embedded.



Região: Norte da Europa | Moeda: Brasil – Real – BRL (R\$) | Exibir preços por: Mês | 1 USD = 4.9448 BRL

### Perguntas frequentes

[Perguntas frequentes sobre os preços do Azure >](#)

- Com que frequência posso alterar o tipo de nó que implantei?
- Como o uso do Power BI Embedded é mostrado na minha fatura?
- Eu preciso comprar licenças adicionais para publicar o BI em um nó do Power BI Embedded?
- Os usuários que exibem o BI publicado no Power BI Embedded precisam ter uma licença separada?**  
Não, os usuários que estão vendo o conteúdo não precisam de licenças do Power BI atribuídas a eles.
- O que acontece se eu pausar meu serviço?
- Qual a relação entre o Power BI Embedded e o serviço do Power BI?

Entretanto, para acessar o Power BI serviço (app.powerbi.com) e conseguir publicar e gerenciar os relatórios publicados, você precisará de licenças PRO.

#### 4. Utilizar a opção de “Publicar na Web” com senha não é seguro?

Utilizar a opção “Publicar na Web” é uma forma de compartilhar relatórios de graça, sem que a pessoa que está visualizando precise ter uma conta ou licença do Power BI.

Ela funciona muito bem quando você precisa compartilhar relatórios que contém **dados públicos**, isto é, quando não há preocupação com vazamento de dados.

**A opção “Publicar na Web” não possui nenhuma segurança:** Qualquer pessoa que tenha acesso ao link do relatório, irá visualizá-lo, sem qualquer controle a nível de usuário, como RLS ou OLS, não há necessidade de quem está visualizando ser cadastrado em nenhuma aplicação e não há auditoria para saber quem está visualizando o relatório. Qualquer pessoa poderá estar visualizando os dados da sua empresa e você não saberá quem.

Além disso, como já amplamente divulgado na internet, todos os relatórios publicados desta forma, podem ser acessados através de consultas simples ao Google, mesmo que o link nunca tenha sido publicado em nenhum local.

Mesmo que você tente bloquear o acesso utilizando uma senha para abrir o portal, esse tipo de mecanismo é facilmente quebrado em poucos segundos, utilizando a opção de Developer Tools do navegador e a pessoa terá acesso irrestrito aos dados publicados no relatório, até mesmo as colunas que estão no modelo, mas não estão sendo mostradas no relatório.

#### 5. Para acessar relatórios sem ter licença PRO não é apenas a partir do F64?

Outra dúvida bem comum é com relação ao licenciamento F64/P1.

Usuários podem acessar os relatórios pelo Power BI serviço em um workspace associado à uma capacidade F64 ou acima (ou Premium por Capacidade = P1), utilizando contas gratuitas, sem necessidade de ter contas Pro para cada usuário.

Mesmo utilizando uma capacidade abaixo da F64, com o F2, F4, F8, etc ou uma capacidade do Power BI Embedded, os seus usuários ainda precisarão de ter licenças PRO para acessar os relatórios **pelo Power BI serviço**, ou seja, **NÃO** se aplica para relatórios inseridos em aplicações web.

**Qualquer capacidade do Fabric ou do Power BI Embedded** permite visualizar os relatórios no Power Embedded, e permitir que os usuários visualizem os relatórios utilizando qualquer email, sem precisar nem de ter conta Microsoft e nem nenhuma licença por usuário (PRO ou PPU).

Neste [link aqui](#), a Microsoft mostra que o Microsoft Fabric também pode ser utilizado normalmente para inserir relatórios em aplicações terceiras em qualquer tamanho de capacidade.

## Power BI embedded with Microsoft Fabric Capacities (F SKUs)

Microsoft Fabric capacities allow you to create and share Fabric content and leverage Fabric for your applications. Microsoft Fabric provides all the capabilities required for a developer to extract insights from data and present it to the business user, whether it is within Fabric or embedded in external applications.

Microsoft Fabric capacities come in a wide range of SKUs, each with different resource tiers for memory and computing power, so you can find the SKU that best fits your application needs. Embedding Power BI artifacts is supported with the whole range of F SKUs. Read more about the different available licenses [here](#).

Just like the familiar A SKUs, F SKUs can be used for as long as you want without any commitment. Pricing is regional and billing is made on a per second basis with a minimum of one minute.

Some additional capabilities with F SKUs include:

- Pay as you go with no time commitment.
- You can scale your capacity up or down using the Azure portal.
- You can pause and resume your capacity as needed.

Fabric capacities also offer a lower entry level, which can be ideal for ISVs and smaller organizations looking to explore Microsoft Fabric and embedded analytics with Power BI. Meanwhile, the higher-level F SKUs allow free users to view Shared Power BI items in any workspace that has such a capacity assigned to it.

## 6. É possível criar, editar e publicar relatórios sem conta PRO?

Neste [link abaixo](#), a Microsoft deixa explícito que alteração e criação de relatórios por meio de um portal que utilize o licenciamento do Power BI Embedded, não requer uma licença PRO ou PPU para isso, e por tanto, a alteração e criação de relatórios pelo Power Embedded é totalmente legal e suportada.

### Quem precisa de uma licença Power BI Pro ou PPU (Premium por usuário) para o Power BI Embedded e por quê?

Você precisa de uma licença Power BI Pro ou PPU (Premium por usuário) ou de uma [entidade de serviço](#) para usar APIs REST. Para adicionar relatórios a um workspace do Power BI, um analista precisa de uma licença Power BI Pro ou PPU (Premium por usuário) ou de uma entidade de serviço. Para gerenciar o locatário e a capacidade do Power BI, um administrador precisará ter uma licença Power BI Pro ou PPU (Premium por usuário).

Como o Power BI Embedded permite o uso do portal do Power BI para gerenciar e validar o conteúdo inserido, a licença Power BI Pro ou PPU (Premium por usuário) é necessária para autenticar o aplicativo no PowerBI.com para obter acesso aos relatórios nos repositórios corretos.

No entanto, para a criação/edição de relatórios inseridos dentro do seu aplicativo, o usuário final não precisa ter uma licença Pro ou PPU (Premium por usuário), pois ele não precisa ser um usuário do Power BI.

Por este motivo que o Power Embedded já permite publicar relatórios PBIX do seu computador diretamente para um workspace do Power BI e também criar/editar relatórios pela interface Web, sem precisar ter uma conta PRO.

## 7. Não posso contratar apenas o Fabric, sem o portal do Power Embedded?

A Microsoft disponibiliza a contratação da capacidade do Power BI Embedded ou Fabric pelo Azure, que nada mais é que um recurso que permite gerar uma quantidade ILIMITADA de tokens para embeddar relatórios em aplicações web.

Caso você utilize o portal padrão do Power BI ([app.powerbi.com](https://app.powerbi.com)), você ainda irá continuar no cenário de licenciamento por usuário, onde cada usuário que for publicar ou visualizar relatórios vai precisar de uma licença Pro (ou Premium por Usuário). Ou seja, você estará pagando a capacidade (que é cara) e ainda terá os mesmos custos de contas Pro que você tem atualmente.

Para utilizar o licenciamento de Embedded do Fabric ou do Power BI Embedded, que é diferente de todos os outros tipos de licenciamentos do Power BI, você obrigatoriamente precisa utilizar uma aplicação Web para gerar esses tokens de forma automática e disponibilizar os relatórios para os seus usuários, pois a Microsoft NÃO disponibiliza um portal ou código-fonte de um portal pronto para ser utilizado nesse cenário.

Você pode criar o seu próprio portal, utilizando uma linguagem de programação, onde você vai implementar todo o código para gerenciar usuários e permissões, renderizar os relatórios, criar o layout do site, implementar a segurança, gerenciar o servidor de aplicação, banco de dados, Firewall, corrigir problemas, implementar novas funcionalidades, prever escalabilidade, alta disponibilidade, etc.

Outra opção é contratar um portal já pronto, com tudo isso (e MUITO mais) já criado e pronto para uso, no modelo SaaS (Software As A Service), onde você não tem nenhuma preocupação ou nada para gerenciar, apenas utiliza o sistema, que é atualizado de forma constante e bem frequente.

Esse é o Power Embedded, a plataforma de relatórios mais completa e robusta do mercado, líder em quantidade de clientes e usuários e totalmente compliance e suportada pela Microsoft.

## Instalação do Power Embedded

Para agendar a instalação do Power Embedded e iniciar o período de avaliação de 30 dias, por favor, utilize o link abaixo:

<https://powerembedded.com.br/instalacao>

Para que a instalação seja realizada com sucesso, é necessário a presença de uma pessoa que seja administradora do portal do Azure (<https://portal.azure.com/>) e alguém que consiga acessar as configurações de locatário do Power BI (<https://app.powerbi.com/admin-portal/tenantSettings>).

Sobre as permissões necessárias para a instalação, seguem atividades que serão realizadas no Azure AD (alguém com permissão “Azure Global Administrator” deve executar):

- Criar um aplicativo no AD (Acessar a tela de registros de aplicativos)
- Criar um novo grupo no AD
- Adicionar esse usuário neste grupo
- Criar o recurso do Power BI Embedded ou Fabric pelo Azure (**opcional se for utilizar o Trial do Fabric**)
- Adicionar o Service Principal recém-criado na role “Contributor” no recurso criado (**opcional se for utilizar o Trial do Fabric**)
- Adicionar o Service Principal recém-criado como “Power BI Capacity Administrator” do recurso criado (**opcional se for utilizar o Trial do Fabric**)
- Logar na área administrativa do Power Embedded ([admin.powerembedded.com.br](https://admin.powerembedded.com.br)), autorizar o aplicativo na sua organização (vai abrir um pop-up no primeiro acesso solicitando o consentimento) e criar os primeiros usuários com perfil de Administrador.
- Logar no portal de visualização do Power Embedded ([relatorios.powerembedded.com.br](https://relatorios.powerembedded.com.br)) e autorizar o aplicativo na sua organização (vai abrir um pop-up no primeiro acesso solicitando o consentimento).

Seguem atividades que iremos realizar no portal de Administração do Power BI (alguém com permissão “Fabric Administrador” deve executar):

- Habilitar as configurações abaixo e permitir o grupo do AD criado a utilizar essas configurações:
  1. Inserir conteúdo em aplicativos
  2. As entidades de serviço podem usar APIs do Fabric
  3. As entidades de serviço podem acessar APIs de administrador somente leitura
  4. Aprimorar as respostas das APIs de administração com metadados detalhados
  5. Permitir pontos de extremidade XMLA e analisar no Excel com modelos semânticos locais



- Associar os workspaces ao recurso da capacidade contratada ou da trial (ou criar novos workspaces para migrar em paralelo)
- Adicionar o grupo do AD criado como administrador dos workspaces

#### **Documentação técnica da instalação:**

[Manual de Instalação - Trial do Fabric - Power Embedded](#)

#### **Site principal do Power Embedded:**

<https://powerembedded.com.br/>

**Série de vídeos sobre o Power Embedded, onde mostramos e explicamos cada uma das telas e funcionalidades do sistema:**

<https://powerembedded.com.br/videos>

#### **Calculadora do Power Embedded para estimar o custo da solução para o seu ambiente:**

<https://powerembedded.com.br/calculadora>

## **Período gratuito de 30 dias do Power Embedded**

O Power Embedded é disponibilizado de forma gratuita, por 30 dias, para que você tenha tempo suficiente para testar o sistema, as funcionalidades oferecidas e garantir que ele irá atender e superar as expectativas e necessidades do seu negócio.

Só é iniciada a cobrança da mensalidade do sistema após 30 dias (contados a partir da instalação do sistema), sendo o primeiro pagamento do sistema no 2º mês de uso. A instalação do sistema também só será cobrada caso o cliente formalize que irá permanecer utilizando a plataforma após o período de testes, ou seja, após 30 dias a partir da data de instalação.

E sobre a capacidade do Fabric, a Microsoft está liberando uma avaliação na capacidade F64 de 60 dias gratuitos, para poder testar tanto a parte de embarcar relatórios quanto os outros recursos da plataforma. Sendo assim, toda a sua PoC será 100% gratuita durante os primeiros 30 dias.

## **Como definir a capacidade ideal para sua empresa**

A cobrança da capacidade do Embedded é calculada a nível de segundo pela Microsoft, e convertida para hora para gerar a cobrança final, e o nosso sistema permite definir os períodos de horários, por dia da semana, que o sistema irá ficar ligado e fora desse horário, o próprio sistema já desliga a capacidade automaticamente.

Caso alguém tente acessar o relatório fora desses horários, o sistema poderá ligar automaticamente para permitir que visualizem os relatórios e irá desligar automaticamente após um período de inatividade (definido por você).

Para definir qual a capacidade mais indicada do Power BI Embedded ou Microsoft Fabric para o seu cenário, você pode nos enviar a quantidade e o tamanho de cada conjunto de dados do Power BI que será importado para a plataforma para termos uma estimativa de qual capacidade mais adequada para o seu cenário, mas iria te gerar um trabalho grande pra fazer esse levantamento e seria apenas uma **estimativa**, pois existem vários outros fatores que influenciam no uso da capacidade além só do tamanho, como complexidade do modelo, relacionamentos, complexidade das medidas e muitos outros fatores.

Entretanto, **o melhor caminho** seria utilizando o período de 60 dias de avaliação gratuita do Microsoft Fabric, onde poderemos rodar toda a PoC de forma gratuita, fazendo com que os relatórios atuais sejam atualizados e processados por essa capacidade trial gratuita (F64), coletando o uso real dessa capacidade através da análise da carga do seu ambiente atual utilizando o relatório "Fabric Capacity Usage Metrics", disponibilizado pela própria Microsoft, a fim de identificar com muito mais precisão qual capacidade que o seu ambiente necessita.

## Como contratar uma capacidade Fabric ou Power BI Embedded

Caso você não tenha parceiro Microsoft ou gostaria de trocar para a Azure Brasil, empresa recomendada pela Power Tuning e Microsoft Solutions Partner nas categorias AI, Dados e Azure, consegue redução de valor em custos de licenciamento (Office, Windows, SQL Server, Power BI, etc) e redução de custos com Azure.

A contratação é feita pelo portal do Azure, de acordo com o tipo de capacidade que você irá utilizar (Microsoft Fabric ou Power BI Embedded).

O time de suporte do Power Embedded faz todo o suporte e apoio durante a contratação.

Como é o processo de contratação da capacidade, caso optem por contratar com a Power Tuning:

1. Você faz o cadastro com os dados da empresa no site <https://powertuning.com.br/parceria-azure>
2. O time da Azure Brasil vai entrar em contato com você para preparar a documentação para enviar para a Microsoft
3. Uma vez aprovado o cadastro, será criada uma assinatura do Azure no seu tenant (só é cobrado após a criação dos recursos)
4. O time da AzureBrasil vai liberar acesso ao Gerenciamento de Custos (por padrão, vem desativado)
5. O time do Power Embedded faz uma nova análise de capacidade para garantir que realmente vai contratar a capacidade ideal pro seu ambiente
6. Nessa mesma reunião, já ajudamos vocês a contratar o Fabric, configurar no Power Embedded e atribuir essa capacidade em todos os workspaces

Benefícios de ter a Azure Brasil como sua parceira de Cloud:

1. **Pagamentos via boleto** ao invés de cartão de crédito. Na modalidade de pagamento via cartão de crédito, caso seja o cenário da sua empresa atualmente (contratando direto com a Microsoft só consegue pagar com cartão), você paga 6.38% de IOF adicionais em cima do valor total do consumo.
2. **Geração de Nota Fiscal** dos recursos e serviços contratados junto ao Azure. Quando você contrata direto com a Microsoft, recebe apenas uma invoice, não recebe Nota Fiscal.
3. **Nós calculamos os impostos e já incluímos no boleto.** Quando você contrata direto com a Microsoft, você é que tem que calcular os impostos (PIS, COFINS, etc) e pagá-los separadamente.
4. **Somos especialistas em Desenvolvimento e Dados**, então fazemos toda uma análise e consultoria durante a contratação de recursos, não apenas vendemos a licença.
5. **Acesso ao Gerenciamento de Custos e a Cobrança.** Prezamos pela transparência e por isso, nossos clientes têm acesso para acompanhar os custos de todos os recursos pelo portal do Azure em tempo real.
6. **Suporte Premier Microsoft 24x7** em caso de problemas em algum produto ou no Azure, você terá atendimento prioritário com o time de Engenheiros da Microsoft, sem nenhum custo adicional.
7. **Licenças mais baratas.** Vendemos licenças Microsoft de Windows, Office 365, Power BI, Fabric, SQL Server e outras, com valores muito mais acessíveis. Power BI? R\$ 51,00 por mês. Office 365 E1? R\$ 51,00 por mês.

A Azure Brasil trabalha bastante em otimização dos custos com Azure e licenciamento e disponibilizamos ferramentas, sem nenhum custo, que fazem uma série de análises para redução dos custos dos recursos já criados:

1. **Automações para desligar recursos em horários pré-definidos**
2. **Análise de uso de instâncias reservadas** para reduzir custos em até 70%
3. **Análises de sub-utilização de recursos**, podendo reduzir a capacidade para economizar
4. **Análises de desvios no padrão de gastos de hora em hora**, para evitar sustos quando chegar a fatura. Qualquer mudança significativa no seu consumo, vamos te avisar.
5. **Deteção de invasão** ao analisar recursos criados em regiões fora do padrão

## Referências

- [Site do Power Embedded](#)
- [Documentação do Power Embedded](#)
- [Calculadora de Economia do Power Embedded](#)
- [FAQ – Perguntas mais frequentes](#)
- [Vídeos de Tutoriais de Uso](#)
- [Novidades do Power Embedded](#)



- [Conheça o licenciamento Fabric e Embedded](#)
- [Como utilizar a API e integrar o Power Embedded na sua Aplicação](#)
- [Preciso de consultoria de DBA / BI / Analytics / Engenharia de dados](#)
- [Agende sua instalação e inicie o teste de 30 dias gratuitos](#)