



Associação Propagadora Esdeva
Centro Universitário Academia –
UniAcademia
Curso de Engenharia de Software e Sistemas de
Informação
Projeto de Extensão – Artigo

Aplicação do Azure AD B2C: Um Estudo Prático

Gabriel Mazilão Ferreira da Silva¹

Centro Universitário Academia, Juiz de Fora, MG

Gabriel Monteiro da Fonseca²

Centro Universitário Academia, Juiz de Fora, MG

Gustavo Sobreira Pinto³

Centro Universitário Academia, Juiz de Fora, MG

Jhonathan Meireles de Oliveira⁴

Delage, Juiz de Fora, MG

Tassio Ferenzini Martins Sirqueira⁵

Centro Universitário Academia, Juiz de Fora, MG

Linha de Pesquisa: Engenharia de
Software

RESUMO

No mundo atual, os bens mais importantes que qualquer empresa pode ter são os dados de seus clientes, através do estudo devido dos dados podemos gerar diversas informações que podem influenciar nas tomadas de decisão do consumidor e da própria empresa. Por conta dessa importância é comum que pessoas mal intencionadas tentem obter esses dados de forma ilegal, para dificultar esses vazamentos diversas leis foram criadas em diferentes partes do mundo, mesmo assim, casos como o Yahoo (2013), Target (2013), Equifax (2017), não são casos isolados, diversas outras empresas também já tiveram falhas na segurança de seus dados. Ainda não possuímos um sistema totalmente seguro, mas através desses erros novas tecnologias estão sendo criadas. Visando aumentar a segurança, empresas como Microsoft, Google e Facebook, entre outras gigantes da tecnologia, oferecem uma opção de login único (*single sign on*), onde dados de seus usuários ficam segurados por essas empresas, onde entende-se que investem mais em

¹ Discente do Curso de Engenharia de Software do Centro Universitário Academia – UniAcademia.

E-mail: gabriel.silva@delage.com.br.

² Discente do Curso de Engenharia de Software do Centro Universitário Academia – UniAcademia.

E-mail: gabriel.fonseca@delage.com.br.

³ Discente do Curso de Sistemas de Informação do Centro Universitário Academia – UniAcademia.

E-mail: gustavo.pinto@dalege.com.br

⁴ Ex-Discente do Curso de Sistemas de Informação do Centro Universitário Academia – UniAcademia.

E-mail: jhonathan.oliveira@delage.com.br.

⁵ Docente do Curso de Engenharia de Software e Sistemas de Informação do Centro Universitário Academia. Orientador.

E-mail: tassio@tassio.eti.br

proteção de dados. Este artigo mostra uma forma de aumentar a segurança de aplicações Web através do uso de tecnologias como as do Azure AD B2C.

Palavras-chave: Azure AD B2C, Tecnologia, Segurança, SSO, JWT

1 INTRODUÇÃO

Segundo a matéria publicada no Jornal Opção, cerca de 30 milhões de senhas foram vazadas no Brasil apenas em 2022, este problema se deu principalmente por conta de usuários salvarem senhas em navegadores, sendo o Google Chrome o que mais teve casos de vazamentos, na tentativa de facilitar o login em diversos sistemas, a segurança desses dados foi afetada.

Neste artigo iremos expor o uso de uma ferramenta que busca manter a comodidade de não precisarmos decorar dezenas de senhas diferentes para cada sistema que entrarmos, mantendo a segurança dessas senhas através de uma tecnologia de login único, também chamado de SSO (Single Sing-On), onde as senhas de usuários não ficam vagando pela rede, como o login único, o usuário cria apenas uma vez seu login e senha e este será usado para logar na plataforma provedora do SSO.

Existem diversos provedores de SSO pelo mercado, tais quais a AWS, Google Identity, porém a ferramenta que iremos abordar neste artigo será o Azure AD B2C, por conta de toda a integração com o ambiente Microsoft, presente no Azure AD B2c e pela confiança que seu antecessor o Azure AD traz consigo.

Mas na prática quais são as vantagens de se ter um login único? Digamos que queremos entrar no sistema da empresa X e para isso, criamos um login e senha, esta empresa não é uma empresa voltada a área de tecnologia e não sabe dos perigos dos vazamentos de dados, por isso não investe na segurança de seus sistemas, caso alguma pessoa tente invadir o sistema, o nível de dificuldade será baixo, com isso o invasor terá acesso a todas as informações dos usuários, incluindo login e senha.

Segundo os resultados de uma pesquisa realizada pela PSafe, 5 em cada 10 brasileiros utilizam a mesma senha em diferentes locais da web, o que resulta em cerca de 67 milhões de pessoas. Então, caso um login seja vazado por essa empresa X, o invasor pode entrar em diversos outros locais e obter mais dados pessoais.

Então o mais seguro seria essa empresa X deixar o sistema de segurança da empresa nas mãos de empresas que entendem e constantemente investem em segurança da informação e é nesta parte que o Azure AD B2C aparece, com ele o usuário da aplicação pode logar com sua conta Microsoft, GitHub, Twitter, Paypal, entre outros, de forma que seu usuário e senha não sejam sequer vistos pela empresa X, de forma que será mostrado mais a frente. Oferecendo a essa empresa maior segurança, confiança e escalabilidade em seus sistemas.

Através do uso da ferramenta, podemos contar com a autenticação de dois fatores da própria Microsoft em qualquer App ou site, o Azure AD B2C traz consigo

anos de experiência e confiabilidade geradas pelo Microsoft AD, seu antecessor, comumente usados em empresas de diversos setores.

O Azure B2C é uma solução abrangente para gerenciamento de identidade e acesso, fornecendo recursos avançados de autenticação, suporte a SSO e integração com diversos provedores de identidade. Ele oferece uma opção segura, escalável e confiável para empresas que desejam proteger as informações dos usuários e proporcionar uma experiência de login conveniente.

Além desta introdução, na seção 2 abordaremos com mais detalhes como funciona a plataforma Azure com foco no Azure AD B2C, junto a ela uma explicação detalhada sobre SSO e JWT, duas soluções que andam juntas quando o assunto é segurança de dados e login único. Mostraremos como aplicar conceitos de SSO em qualquer aplicação que rode em nuvem, assim como explicaremos a forma de criptografia do JWT.

2 REFERENCIAL TEÓRICO

O Azure AD B2C é uma tecnologia lançada pela Microsoft no ano de 2016, utilizada em diversos sistemas. Mesmo após sete anos após seu lançamento, ainda existem poucos materiais em português sobre o tema.

A fim de sanar parte dessa carência de conteúdo, este artigo faz parte de um estudo feito por nós da Delage, buscando a implementação em nossos sistemas.

2.1 PLATAFORMA AZURE

Assim como AWS, Google Cloud, entre outras, Azure é a plataforma em nuvem mantida pela Microsoft, nela podemos escolher diversas opções de produtos, de máquinas virtuais à controle de versionamento, segundo a própria Microsoft, na plataforma podemos escolher mais de 200 produtos, todos eles com a segurança e confiança Microsoft.

Com as novas políticas da Microsoft para sistemas cada vez mais abertos, a plataforma não se limita a apenas ferramentas para Windows, é possível executar a grande maioria das soluções em qualquer sistema operacional. É aconselhável testar a solução antes de aplicá-la na empresa, para isso o Azure nos proporciona um experimental de 200 dólares, durante 30 dias, o que proporciona uma melhor análise da plataforma.

2.2 SINGLE SIGN ON (SSO)

Como o avanço da rede no mundo moderno, tornou-se uma tarefa crucial a proteção de dados pessoais, uma vez que parte de nossas vidas estão dentro dos servidores de uma infinidade de empresas, governos, etc. Pensando na segurança desses dados diversas leis criadas, a fim de proteger o usuário de uma exposição

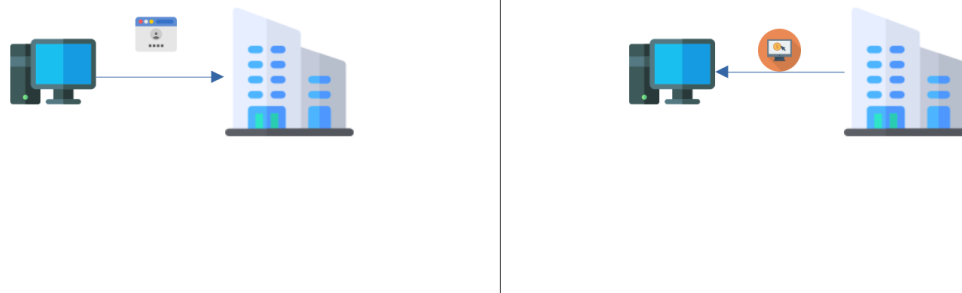
desnecessária, quando uma empresa séria precisa de capturar um dado, devem ser feitas três perguntas: “é legal?”, “é moral?” e “é necessário?”.

Algumas empresas, ao se perguntarem se é necessário armazenar o login, mesmo que de imediato responda que sim, o login não é algo crucial a se ter nos bancos de dados de uma empresa, não é possível extrair informações do cliente de maneira moral através de dados de login. São dados que se fazem úteis para apenas um propósito, garantir o login seguro do usuário, porém ficar mandando logins e senhas diretamente na rede, conforme a Figura 1, em qualquer lugar não parece ser uma boa forma de estar seguro, uma vez que já foi dito 50% dos brasileiros usam as mesmas senhas, então mesmo que sua aplicação seja segura, uma falha de segurança de outro local pode comprometer o usuário severamente em seu sistema.

Por conta de falhas como essa o SSO existe, ele consiste em registrar o usuário em grandes plataformas, como Google, Microsoft, Facebook, entre outras, onde elas fazem a segurança de login destes usuários e quando ele tentar logar em outra aplicação o login é redirecionado e autenticado por essas plataformas.

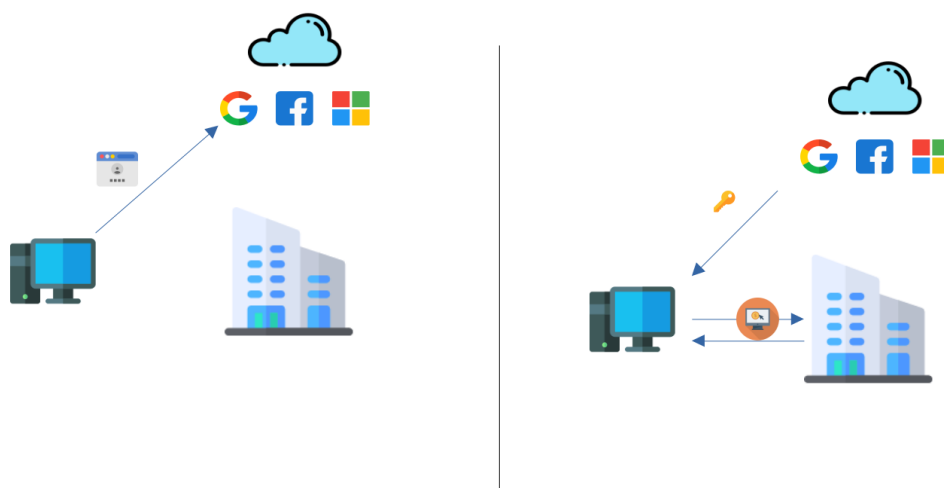
Digamos que o usuário queira registrar-se em uma aplicação utilizando o Facebook, então caberá ao Facebook fazer a segurança desses dados, mesmo que o usuário tenha dados vazados em plataformas X ou Y, estes não afetarão em sua plataforma. Com exceção de uma falha na segurança no próprio Facebook, o que tende a ser mais difícil do que uma plataforma de menor investimento.

Figura 1 - Login convencional



Fonte: autoral.

Figura 2 - Login utilizando SSO



Fonte: autoral.

Caso sua aplicação adote o modelo da Figura 2, antes que o usuário possa ter acesso a qualquer serviço de seu fornecimento, será necessário fazer login em uma dessas plataformas.

Com o login efetuado por exemplo nos serviços do Google através de seu e-mail, o usuário receberá uma chave (token), conforme ilustra a Figura 2, com esse token em sua máquina a cada solicitação de um novo serviço, ele será passado junto à URL, de modo que o usuário nunca fique logado da aplicação, em toda requisição será necessário passar a chave junto a solicitação, para verificação de identidade do usuário, evitando ataques como *Cross-site Request Forgery* (CSRF), uma vez que não há sessão a ser falsificada.

Esta chave armazena diversas informações importantes do usuário, como grupos, permissões etc., geralmente este tipo de token está no formato JWT que será o próximo tópico deste artigo.

2.3 JSON WEB TOKEN (JWT)

O JWT é um padrão de troca de informações entre sistemas (RFC 7519), que ganhou notoriedade pelo fato da facilidade de transmissão, recepção e sua segurança. Seu formato é simples e reconhecido por grande parte dos sistemas, uma vez que os dados são enviados pelo body da requisição, no formato Json, substituindo o uso do formato XML.

Uma de suas grandes vantagens é a não manutenção de estado (*stateless*), não há login, toda requisição contém uma chave privada que permite que o usuário cumpra ou não determinada tarefa, a depender do grupo de usuário em que ele esteja e suas respectivas permissões atribuídas, através do serviço Auth0.

Este tipo de token, se divide em três partes, header, payload e verify signature.

Header: Contém informações sobre o tipo de algoritmo de criptografia utilizado na requisição, conforme mostra a Figura 3.

Figura 3 - Cabeçalho JWT

```
HEADER: ALGORITHM & TOKEN TYPE

{
  "alg": "HS256",
  "typ": "JWT"
}
```

Fonte: autoral.

Payload: Aqui são passados todos os dados referentes ao conteúdo da requisição, como usuário, grupos, roles, ou qualquer dado que seja importante para aplicação não se limitando a conteúdos referentes ao usuário a Figura 3.1 ilustra como é feita a escrita de um conteúdo no payload.

Figura 3.1 - Conteúdo JWT

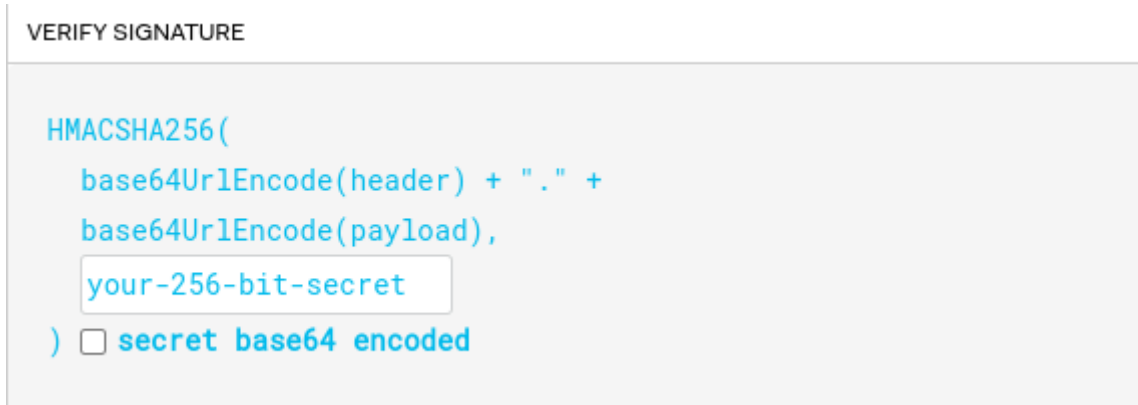
```
PAYLOAD: DATA

{
  "sub": "1234567890",
  "name": "Gustavo Sobreira",
  "group": "Desenvolvedor"
}
```

Fonte: autoral.

Verify signature: Nesta parte é passado a assinatura da requisição, uma assinatura que é formada a partir da combinação dos *hashes* referentes ao header, payload é a chave secreta da aplicação, ou seja, qualquer modificação em um desses lugares, faz uma grande alteração, invalidando o token, a Figura 3.2 ilustra como é feita essa combinação.

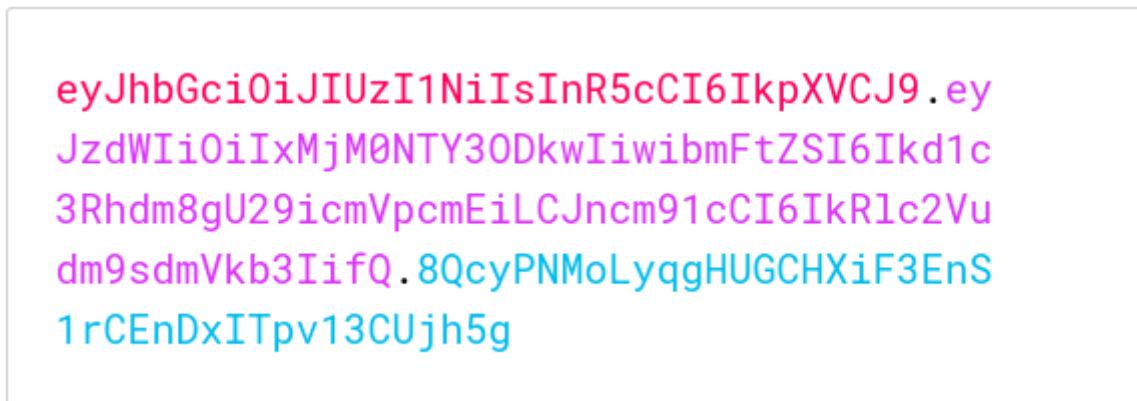
Figura 3.2 - Assinatura JWT



Fonte: autoral.

Token: Como resultado das combinações dos tópicos anteriores, temos o token, que será a forma de envio entre um ponto a outro. Veja a Figura 3.3.

Figura 3.3 - Token JWT



Fonte: autoral.

Todas as imagens referentes ao JWT foram tiradas do site JWT.io, caso não esteja familiarizado com este padrão é recomendado acessá-lo e fazer seus próprios testes.

2.3.1 Trabalhos relacionados

Em uma abordagem mais profunda ao payload, pode-se notar na Figura 3.3 na cor rosa (após o primeiro ponto) a criptografia referente ao payload, feita em base 64, existe uma série de regras a serem seguidas para que o JWT funcione conforme o previsto, algumas nomenclaturas devem ser seguidas.

Dado que nosso objetivo ao utilizarmos o JWT é conseguir nos comunicar com outras aplicações, não basta adicionar várias informações que por falta de uma convenção não serão capturadas pelo outro ponto, para isso existem algumas palavras chaves que devem ser usadas no seu JWT.

“A informação de “sub” que define do subject do token, isso é, o número de identificação do sujeito para quem o token pertence. Já a informação de “iss” é o issuer que

foi definido para identificar o nível de acesso daquele usuário à aplicação.” (Souza Montanheiro et al. 4)

3 IMPLEMENTAÇÃO DO AZURE AD B2C

Com os conceitos necessários para o entendimento de como funciona o SSO, podemos buscar implementar esta solução em uma aplicação real. Antes de tudo será necessário escolher uma plataforma que dê suporte ao SSO, conforme dito na introdução, pode-se usar AWS, Google Cloud, entre outras, porém decidimos explorar a ferramenta da Microsoft Azure AD B2C, por conta da integração com o ambiente Microsoft. Vale ressaltar que este artigo foi escrito no ano de 2023 e caso haja alguma modificação em atualizações futuras, e algo pare de funcionar, procure a documentação oficial da Microsoft em Azure.

3.1 CONFIGURAÇÕES AZURE AD B2C

Para ter acesso ao Azure AD B2C, primeiramente será necessário criar uma conta na plataforma Azure da Microsoft. Com a conta criada, deve-se criar um diretório, onde o Azure AD B2C esteja habilitado.

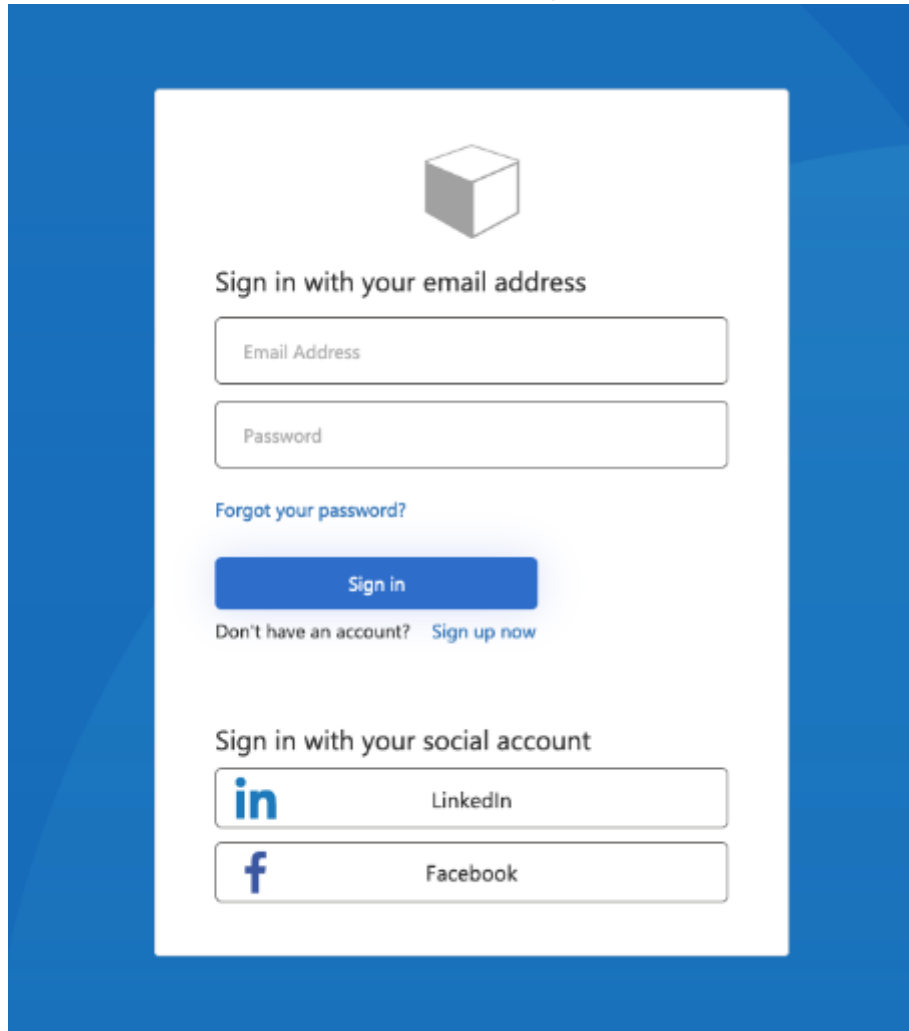
Configure as políticas de acesso de acordo com sua necessidade, habilitando somente o que sua solução precisar, para maior segurança.

3.2 PROVEDORES DE IDENTIDADE

Atualmente o Azure AD B2C nos permite utilizar qualquer provedor de identidade que tenha suporte aos protocolos OAuth 1.0, OAuth 2.0, OpenID Connect e SAML. Isso significa que nossos APPs possibilitam login com mais de 20 provedores diferentes, dentre eles Facebook, Google, GitHub.

Para que o usuário tenha todas estas opções, basta cadastrar cada uma delas na aplicação, podendo ter apenas uma, conforme a necessidade.

Figura 4 - Autenticação



The image shows a login interface with a blue background. At the top center is a 3D cube icon. Below it, the text 'Sign in with your email address' is displayed. There are two input fields: 'Email Address' and 'Password'. Below these fields is a link 'Forgot your password?'. A blue 'Sign in' button is positioned below the link. Underneath the button, the text 'Don't have an account? Sign up now' is shown. Further down, the text 'Sign in with your social account' is displayed. There are two buttons for social login: one with the LinkedIn logo and the text 'LinkedIn', and another with the Facebook logo and the text 'Facebook'.

Fonte: Microsoft.

Nesta aplicação acima podemos notar que temos três formas de login, o padrão, onde primeiramente deve-se criar usuário, para depois entrar através do login e senha, mantendo a aplicação logada e tem também a opção de utilizar-se do SSO, fornecido pelo Facebook e LinkedIn.

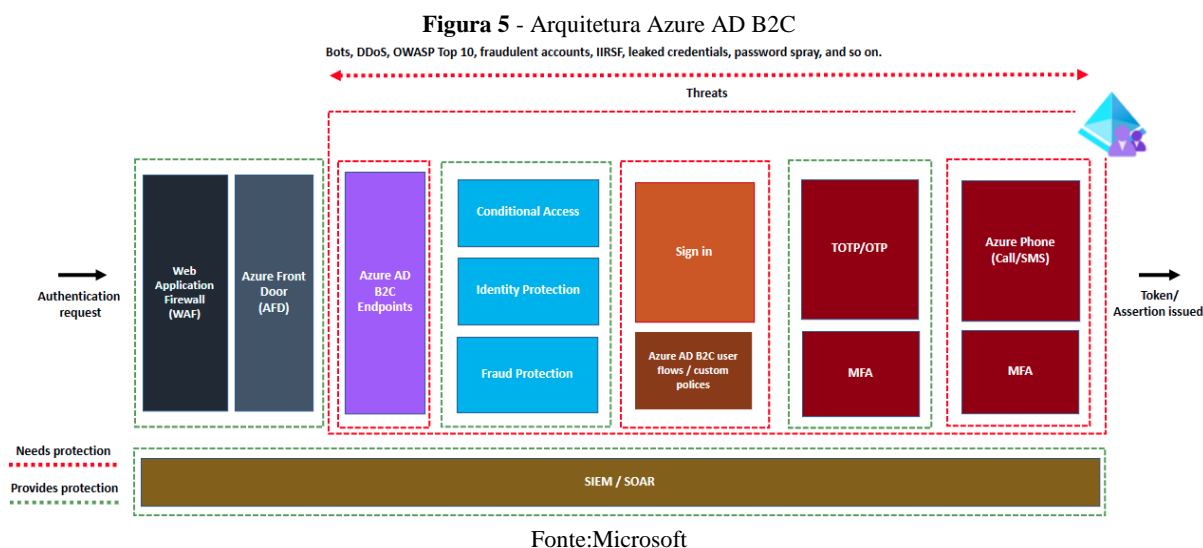
3.3 CONFIGURAÇÃO DE SEGURANÇA

Também pode-se configurar soluções para a segurança na entrada da aplicação, neste ponto é necessário entender dois conceitos de segurança, o Firewall de Aplicativo Web (WAF) e o Azure Front Door (AFD), que serão usados para segurar pontos de extremidade de autenticação e para pontos de extremidade de sua API externa.

- **Firewall de Aplicativo Web (WAF):** usado para evitar ataques como SQL injection, cross-site scripting, DDoS, entre outros. Atua como um filtro entre o

que é passado do usuário para o servidor, onde as impurezas são tratadas e somente o que não prejudicará a aplicação, chegará ao servidor.

- **Azure Front Door (AFD):** serviço que atua como um balanceador de carga para sua aplicação, além de acelerar sua aplicação, também a protege, pois nele é possível habilitar o acesso por certificados.



Desta forma a Microsoft consegue dificultar que ataques entre o usuário e o Azure AD B2C ocorra, adicionando uma camada de segurança no login antes mesmo que ele ocorra.

4 CONTROLE DE USUÁRIOS

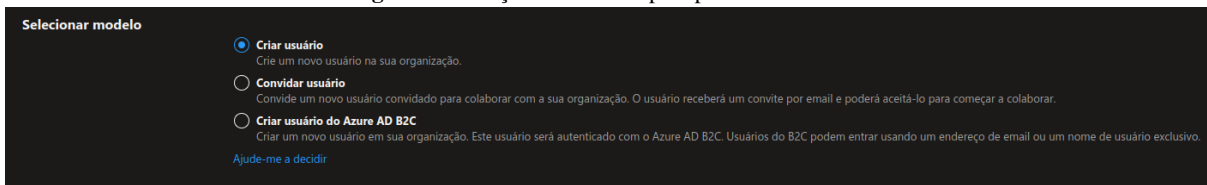
Não adianta adicionar dezenas de camadas de segurança caso toda pessoa que faça login tenha acesso ilimitado a todas requisições da solução, mesmo sendo uma solução pública é necessário que por exemplo o usuário X não possa alterar algo do usuário Y, sem seu consentimento, por simplesmente ter entrado pelo Facebook, para restringir esse acesso o Azure AD B2C permite a criação de usuários internos, onde é possível de maneira arbitrária dar ou retirar permissões de usuários a depender de suas responsabilidades.

Para controle desses usuários, há a opção de controle direto na plataforma Azure, porém existe também uma forma de gerenciar o Azure AD B2C por uma API externa, podendo gerar sua própria interface.

4.1 CRIANDO USUÁRIO PELA PLATAFORMA AZURE

Para registrar um novo usuário no Azure AD B2C usando a própria plataforma Azure, temos as seguintes opções:

Figura 6 - Criação de Usuário pela plataforma Azure



Fonte: autoral.

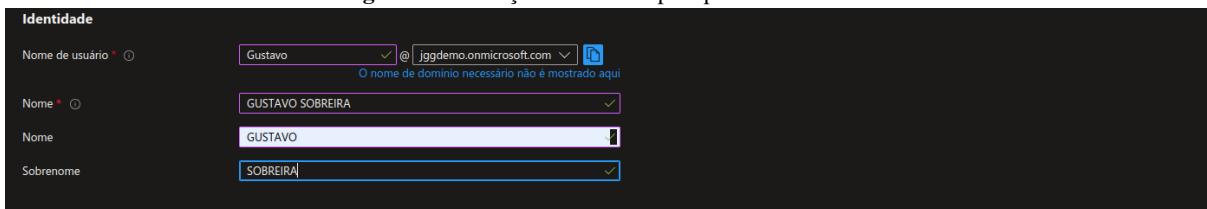
Nesta opção, pode-se criar um usuário do zero, fornecendo dados básicos como nome, e-mail, endereço, um formulário de criação padrão, o que faz essa opção ser bastante utilizada nas automações via código.

Na segunda opção, o usuário recebe um link onde ele mesmo pode criar seu usuário no AD B2C, sendo uma boa opção para negócios onde a participação na solução seja algo mais livre, porém temos o controle de qual conteúdo o usuário terá acesso.

Por fim, a última opção nos dá a liberdade de modificarmos os campos de usuários, tendo dados importantes que normalmente não seriam pedidos.

Após selecionarmos uma das opções teremos a tela de configurações, logo abaixo, onde coloca-se dados básicos do usuário:

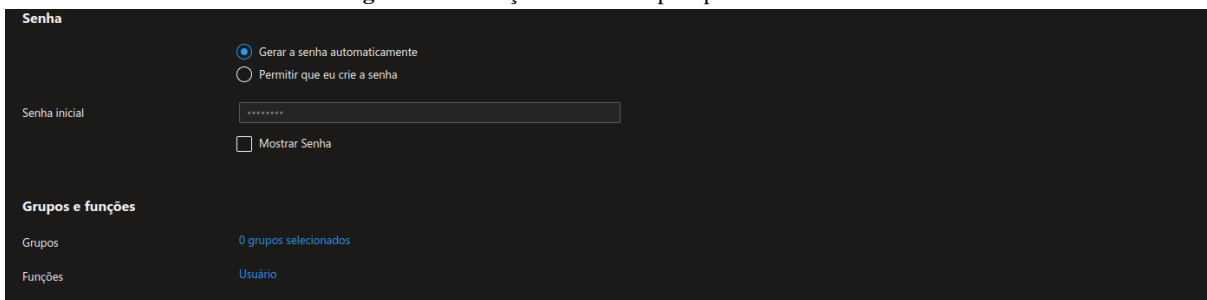
Figura 6.1 - Criação de Usuário pela plataforma Azure



Fonte: autoral.

No campo de “Senha” podemos gerar uma senha, ou pedir que a própria Microsoft gere a senha para o usuário, já no campo “Grupo e Funções”, há a possibilidade de restringirmos o acesso pelas funções e grupos de usuário, mostrando ao usuário somente o que ele pode ter acesso, diminuindo falhas de segurança e vazamento de dados.

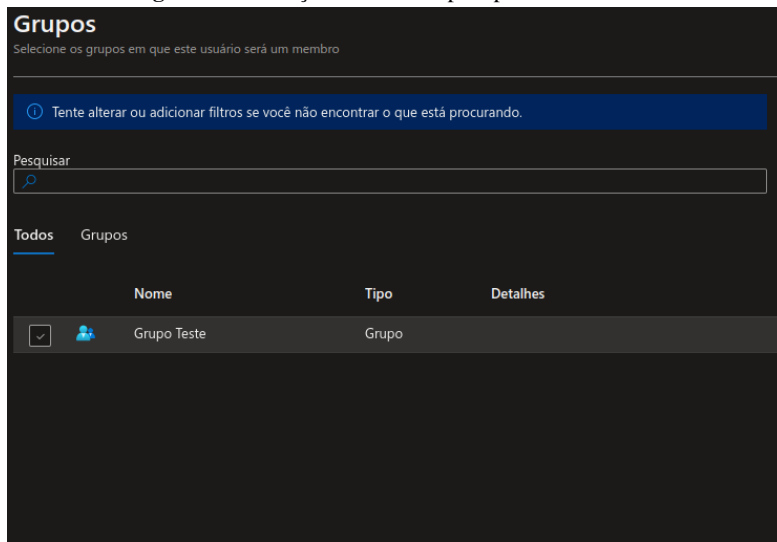
Figura 6.2 - Criação de Usuário pela plataforma Azure



Fonte: autoral.

Para selecionar um grupo ou uma função ao usuário, basta clicar no link a direita e a seguinte tela abrirá:

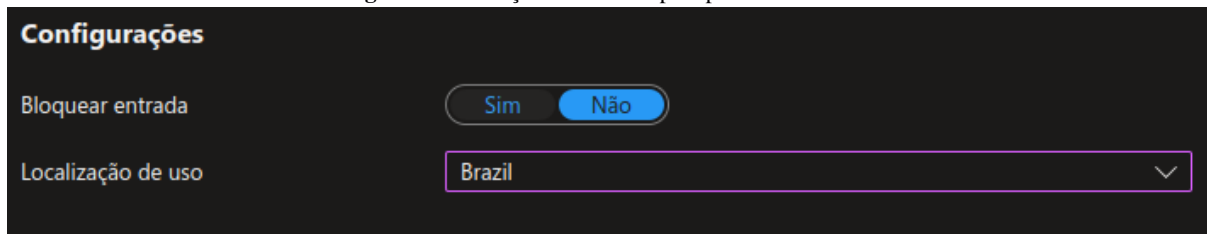
Figura 6.3 - Criação de Usuário pela plataforma Azure



Fonte: autoral.

Além dessas configurações, podemos também criar restrições geográficas, restringindo o uso de VPNs (Rede Privada Virtual).

Figura 6.4 - Criação de Usuário pela plataforma Azure



Fonte: autoral.

Com essa configuração em “Sim” caso o usuário tente acessar a aplicação fora do país indicado, o login não será efetuado. Pois somente IPs brasileiros serão permitidos.

Após isso basta criar o usuário, e o resultado será o seguinte:

Figura 6.5 - Criação de Usuário pela plataforma Azure

	Nome	Nome de usuário	Tipo de usuário	Fonte
<input type="checkbox"/>	AD admin	admin@jgdemo.onmicrosoft.com	Member	Azure Active Directory
<input type="checkbox"/>	GM Gabriel Monteiro	gfonseca3117_gmail.com#EXT#@jgdemo.onmicrosoft.com	Member	Microsoft Account
<input type="checkbox"/>	Gustavo Pinto	gustavo.pinto_delage.com.br#EXT#@jgdemo.onmicrosoft.com	Guest	External Azure Active Directory
<input type="checkbox"/>	Jhonathan Oliveira	jhonathan.oliveira_delage.com.br#EXT#@jgdemo.onmicrosoft.co...	Guest	External Azure Active Directory
<input type="checkbox"/>	LN unknown	jhon4than1995@gmail.com	Member	Azure Active Directory
<input type="checkbox"/>	LN unknown	gustavosobreira1@gmail.com	Member	Azure Active Directory
<input type="checkbox"/>	LN unknown	jhon4than_jf@hotmail.com	Member	Azure Active Directory
<input type="checkbox"/>	LN unknown	gfonseca3117@gmail.com	Member	Azure Active Directory
<input checked="" type="checkbox"/>	GS GUSTAVO SOBREIRA	Gustavo@jgdemo.onmicrosoft.com	Member	Azure Active Directory

Fonte: autoral.

4.2 CRIANDO USUÁRIO POR API EXTERNA

Repare na imagem 6.5, note que dois usuários tem a “Fonte” diferente dos demais, o terceiro e quarto usuário possuem um “External” antes do “Azure..” isso nos mostra que esse usuário não foi criado dentro da plataforma Azure. Conforme dito no tópico anterior na primeira parte, podemos criar usuários por meio de API’s.

Através das API’s temos uma forma mais prática de criação de usuários no Azure AD B2C, pois basta configurarmos uma vez e podemos disponibilizar esta API em diversos contextos.

Para exemplo, utilizamos a linguagem C#, mantida pela própria Microsoft, porém é possível criá-la em Python, Java, PHP, entre outras.

Figura 7.1 - Criação de usuário no Azure AD B2C, via API

```
[HttpPost("create")]
public async Task<IActionResult> CreateUserAsync([FromBody] UserModelB2CIdentity userRequest)
{
    if (!ModelState.IsValid)
    {
        return BadRequest(ModelState);
    }

    var createdUser = await _graphService.CreateGraphApiUserAsync(
        userRequest.DisplayName,
        userRequest.Email,
        userRequest.Password
    );

    if (createdUser == null)
    {
        return BadRequest("Não foi possível criar o usuário.");
    }

    return CreatedAtRoute("GetUserById", new { id = createdUser.Id }, createdUser);
}
```

Fonte: autoral.

Os campos de usuários são definidos pela (Model UserModelB2CIdentity), são recebidos via body, geralmente em formato Json, com os dados desse usuário, é possível criar um objeto através da biblioteca MsGraphServer, onde nós a nomeamos como _graphServer, na injeção de dependências. Esta biblioteca possui o método CreateGraphApiUserAsync, onde passamos os dados de usuário e ela cria um usuário no Azure AD B2C, além dos dados que criamos na imagem acima, também é possível criar outros campos, como os demonstrados na documentação da biblioteca.

Figura 7.2 - Criação de usuário no Azure AD B2C, via API

```
var requestBody = new User
{
    AccountEnabled = true,
    DisplayName = "Adele Vance",
    MailNickname = "AdeleV",
    UserPrincipalName = "AdeleV@contoso.onmicrosoft.com",
    PasswordProfile = new PasswordProfile
    {
        ForceChangePasswordNextSignIn = true,
        Password = "xWwvJ]6NMw+bWH-d",
    },
};
var result = await graphClient.Users.PostAsync(requestBody);
```

Fonte: autoral.

Desta forma é criado um usuário, que ao fazer o seu primeiro login na plataforma, será imposto uma troca de senha, para que mesmo quem criou esta API, não possa saber a senha de um usuário.

5 CONSIDERAÇÕES FINAIS

Neste artigo, exploramos as funcionalidades, a implementação do Azure B2C num ambiente empresarial e os benefícios que a plataforma oferece. Em sumo, o Azure B2C é uma ferramenta poderosa quando o assunto é segurança, devido principalmente ao SSO e ao Json Web Token que possuem um relacionamento bastante sinérgico, cujo uma passa a confiabilidade através de uma grande empresa e o outro através da criptografia, segundo a própria Microsoft. Além disso, a aplicação fornece soluções potentes para a gestão de identidades e acessos em cenário comercial voltado para o consumidor.

Segundo a Microsoft, na documentação do Azure B2C, entendeu-se que a gestão de identidades no Azure B2C é bastante abrangente e permite a empresa ser bastante versátil na customização do aplicativo para entregar uma interatividade melhor ao cliente, podendo fazer com que a ferramenta possa ser empregada em vários cenários,

No quesito implantação do B2C, pode-se dizer que é uma parte mais simples do projeto, a criação de diretórios e configurações do aplicativo possuem uma interface amigável, permitindo melhor entendimento do processo na documentação, entretanto, a parte do controle de usuários é um pouco mais complicada quando cria-se um usuário via API, devido principalmente a escassez de conteúdo além da documentação oficial.

Sendo assim, conclui-se que é a ferramenta ideal para empresas de grande e pequeno porte que desejam a segurança de seus dados e buscam se destacar no mercado, no entanto é essencial ressaltar que a implementação da plataforma quando bem-sucedida necessita de um bom planejamento e conhecimento das

necessidades específicas da empresa, além de exigir uma curva de aprendizado maior da equipe de desenvolvimento, principalmente se não for familiarizado com os serviços de nuvem da Microsoft

Em última análise, além de simplificar a gestão de identidade de acessos, também proporciona uma base sólida para conquistar a confiança na relação cliente empresa e, com o planejamento devido, o Azure B2C poderá se tornar um pilar para o sucesso das estratégias de negócio.

6 REFERÊNCIAS

France Presse, (2017). **Yahoo afirma que ciberataque de 2013 afetou todas as 3 bilhões de contas de usuário.** Disponível em:

<https://g1.globo.com/tecnologia/noticia/yahoo-afirma-que-ciberataque-de-2013-afetou-todas-as-3-bilhoes-de-contas-de-usuarios.ghtml>

Acessado em: 27/11/2023

Sociedade Brasileira de Varejo e Consumo, (2019). **Invasão histórica na Target o que aprendemos em 5 anos?** Disponível em: <https://sbvc.com.br/invasao-target-cinco-anos/>

Acessado em: 28/11/2023

Ciso Advisor, (2020). **Equifax faz acordo por vazamento de dados, mas prejuízo é bilionário.** Disponível em: <https://www.cisoadvisor.com.br/equifax-faz-acordo-por-vazamento-de-dados-mas-prejuizo-e-bilionario/#:~:text=Entre%20maio%20e%20junho%20de,Struts%20sem%20atualiza%C3%A7%C3%A3o%20de%20seguran%C3%A7a./>

<https://www.cisoadvisor.com.br/equifax-faz-acordo-por-vazamento-de-dados-mas-prejuizo-e-bilionario/#:~:text=Entre%20maio%20e%20junho%20de,Struts%20sem%20atualiza%C3%A7%C3%A3o%20de%20seguran%C3%A7a./>

Acessado em: 28/11/2023

Junior Kamenach, (2023). **Cerca de 30 milhões de senhas foram vazadas no Brasil em 2022, diz levantamento.** Disponível em: <https://www.jornalopcao.com.br/ultimas-noticias/cerca-de-30-milhoes-de-senhas-foram-vazadas-no-brasil-em-2022-diz-levantamento-489026/>.

<https://www.jornalopcao.com.br/ultimas-noticias/cerca-de-30-milhoes-de-senhas-foram-vazadas-no-brasil-em-2022-diz-levantamento-489026/>.

Acessado em: 28/11/2023

__. Provedor de identidade AWS, disponível em: <https://aws.amazon.com/pt/iam/identity-center/>. Acessado em: 28/11/2023

__. Provedor de identidade Google, disponível em: <https://cloud.google.com/identity?hl=pt-br>. Acessado em: 28/11/2023

__. Tilt Uol, (2019). **5 em cada 10 brasileiros usam a mesma senha em diferentes contas na web.** Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2019/11/22/5-em-cada-10-brasileiros-usam-a-mesma-senha-em-diferentes-contas-na-web.htm>.

<https://www.uol.com.br/tilt/noticias/redacao/2019/11/22/5-em-cada-10-brasileiros-usam-a-mesma-senha-em-diferentes-contas-na-web.htm>. Acessado em 28/11/2023

__. Json Web Token, disponível em: <https://jwt.io>. Acessado em: 28/11/2023

___ . Documentação Azure AD B2C, disponível em: <https://learn.microsoft.com/en-us/azure/active-directory-b2c/>. Acessado em: 28/11/2023

___ . Provedores compatíveis com Azure B2C, disponível em: <https://learn.microsoft.com/pt-br/azure/active-directory-b2c/add-identity-provider>. Acessado em 28/11/2023

___ . Imagem da interface, disponível em: <https://learn.microsoft.com/pt-br/azure/active-directory-b2c/customize-ui?pivots=b2c-user-flow>. Acessado em: 28/11/2023

___ . Imagem da Arquitetura Azure AD B2C, disponível em: <https://learn.microsoft.com/pt-br/azure/active-directory-b2c/security-architecture>. Acessado em 28/11/2023

___ . Linguagens suportadas pelo sistema B2C, disponível em: <https://learn.microsoft.com/pt-br/graph/api/user-post-users?view=graph-rest-1.0&tabs=cli>. Acessado em 28/11/2023