Conexão Federada entre Google Workspace e Microsoft 365

Vitor Renato Alves de Brito

Núcleo de Tecnologia da Informação - NTI

Universidade Federal de Alfenas - UNIFAL-MG

vitorrenato.brito@unifal-mg.edu.br

Resumo. *Este artigo examina a necessidade de uso da plataforma Google Workspace como Provedora de Identidade para a plataforma Microsoft 365. Com um sistema interno de gerenciamento de usuários e a plataforma da Google já consolidados na Universidade Federal de Alfenas - UNIFAL-MG e, visando facilitar o acesso à plataforma da Microsoft, decidiu-se por adotar a conexão federada oferecida pela plataforma da Google e a configuração automática de licenças na plataforma da Microsoft por meio de um script PowerShell. O objetivo foi proporcionar aos usuários uma experiência simplificada no uso das ferramentas oferecidas pela plataforma da Microsoft, para o aprimoramento dos processos acadêmicos.*

Abstract. *This article examines the need to use the Google Workspace platform as Identity Provider for the Microsoft 365 platform. With an internal user management system and the Google's platform already consolidated at the Federal University of Alfenas - UNIFAL-MG and, aiming to facilitate access to the Microsoft's platform, it was decided to adopt the federated connection offered by the Google's platform and the automatic licenses configuration on the Microsoft's platform using a PowerShell script. The objective was to provide users with a simplified experience in using the collaborative tools offered by Microsoft's platform, to improve academic processes.*

Introdução

A Universidade Federal de Alfenas - UNIFAL-MG, com mais de cem anos de trajetória como Universidade Pública Federal, enfrentou desafios significativos durante a pandemia de COVID-19, especialmente em 2020. Diante da urgência em proporcionar acesso imediato a ferramentas essenciais para ensino, pesquisa, extensão e trabalho remotos, a Universidade optou por adotar a plataforma Google Workspace (anteriormente conhecida como *G Suite for Education*), na modalidade gratuita, oferecida às instituições de ensino. Toda a gestão da plataforma foi concebida com base na adaptação do Sistema de Gerenciamento de Usuários, desenvolvido internamente e já consolidado. Este sistema garante uma gestão centralizada, integração e sincronização das credenciais de acesso dos usuários usando um servidor LDAP (OpenLDAP) e banco de dados, facilitando o acesso a todos os sistemas e serviços de Tecnologia da Informação e Comunicação (TIC) oferecidos pela UNIFAL-MG.

Em 2023, após consolidar a utilização da plataforma da Google na comunidade acadêmica, a demanda foi pela utilização, também, da plataforma Microsoft 365. Este novo passo foi motivado pela percepção de que a plataforma da Microsoft também

oferece diversas ferramentas que poderiam contribuir significativamente para a melhoria dos processos acadêmicos. Algumas dessas ferramentas já eram utilizadas pela comunidade de forma gratuita, porém, de maneira descentralizada, sem uma gestão adequada, por meio de cadastros pessoais e manuais e, muitas vezes, utilizando licenças incorretas para o perfil de cada usuário.

Diante desse contexto, a utilização da plataforma Google Workspace como Provedora de Identidade (IdP) para a plataforma Microsoft 365, tornou-se não apenas uma resposta às demandas emergentes, mas também uma estratégia proativa para oferecer uma experiência acadêmica mais abrangente e eficaz, utilizando, também, das licenças educacionais gratuitas oferecidas pela plataforma da Microsoft, porém, com uma gestão centralizada, controlada e de forma automática.

Este artigo explora os resultados e benefícios dessa iniciativa, destacando os seus impactos positivos nos processos acadêmicos e administrativos na UNIFAL-MG.

Metodologia

Antes da conexão federada entre a plataforma Google Workspace e a plataforma Microsoft 365, a gestão da plataforma da Microsoft era realizada por um setor externo ao Núcleo de Tecnologia da Informação - NTI, de forma manual e sem suporte técnico oficial do NTI. Nesse cenário, não havia um controle adequado sobre os usuários nem sobre a atribuição de licenças, resultando em um processo desorganizado e sujeito a inconsistências.

A ideia de utilizar o Google Workspace como IdP para a plataforma da Microsoft começou a ganhar relevância com o surgimento da demanda pela utilização das ferramentas da Microsoft pela comunidade acadêmica. Nesse contexto, optou-se por uma abordagem que fosse simples e amigável ao usuário e, ao mesmo tempo, reduzisse a necessidade de desenvolvimento ou alterações substanciais nos sistemas internos da Universidade, que já estavam adaptados e adequados para a plataforma Google Workspace.

Um dos pontos principais da conexão federada entre as plataformas foi a implementação do provisionamento automático de usuários da plataforma Google Workspace para a plataforma Microsoft 365, deixando a plataforma da Google como IdP, fazendo o controle de usuários e credenciais de acesso e possibilitando o uso do login único. Essa abordagem permitiu uma autenticação única e simplificada para os usuários, facilitando o acesso à plataforma da Microsoft por meio de autenticação federada via plataforma da Google.

O processo também envolveu a programação de um *script PowerShell* para automatizar a configuração de licenças, conforme o perfil de cada usuário, baseado no domínio/subdomínio do seu e-mail. Decidiu-se pela programação de um *script PowerShell* que fosse executado algumas vezes por semana (ou em ocasiões esporádicas) e que fizesse a configuração das licenças disponíveis para cada usuário. A adoção do *PowerShell* se deu devido a sua capacidade na automação de tarefas via comandos e encadeamento (*pipelines*), por interagir diretamente com as Interfaces de Programação de Aplicações (APIs) da plataforma Microsoft 365 e utilizando uma conexão segura.

O passo inicial para o funcionamento da implementação foi a correção dos domínios/subdomínios utilizados pela UNIFAL-MG na plataforma Microsoft 365, para que refletissem o controle do NTI sobre os mesmos. O domínio unifal-mg.edu.br, utilizado por docentes, técnicas e técnicos administrativos, teve seu DNS corrigido e foi verificado através de alterações nos servidores da UNIFAL-MG, o subdomínio sou.unifal-mg.edu.br, utilizado por discentes, que inicialmente não havia sido cadastrado na plataforma por iniciativa do NTI e estava sendo controlado por pessoa externa não autorizada, teve que ser recuperado e também teve seu DNS corrigido e foi verificado e, o domínio colab.unifal-mg.edu.br, utilizado por colaboradoras e colaboradores, foi cadastrado e verificado corretamente. Como particularidade da plataforma Microsoft 365, o domínio padrão não pode ser um domínio federado, portanto, foi utilizado um subdomínio desativado (discentes.unifal-mg.edu.br) como domínio padrão na plataforma, para que o domínio unifal-mg.edu.br pudesse ser configurado.

O próximo passo foi a instalação do aplicativo Microsoft Office 365 no console de administração da plataforma Google Workspace e a sua configuração inicial padrão e ativação para todos os usuários de todas as unidades organizacionais da plataforma. A ativação do provisionamento automático de usuários é o passo final desta etapa e é feito, ainda, na tela do aplicativo Microsoft Office 365. Neste ponto, foi necessário estabelecer uma conexão com a plataforma da Microsoft, utilizando um usuário com funções de administrador e que fosse diferente de qualquer usuário existente na plataforma Google Workspace. Atentou-se, também, para o mapeamento correto dos atributos obrigatórios e para as ações a serem executadas na plataforma Microsoft 365 quando os usuários forem suspensos ou removidos da plataforma Google Workspace. Após a configuração, todos os usuários existentes, de todos os domínios em comum entre as plataformas, foram removidos da plataforma Microsoft 365 e passaram a ser provisionados pela plataforma Google Workspace, automaticamente. Após a configuração, foi feito o download dos metadados do IdP, contendo informações necessárias para a finalização do processo via comandos do *PowerShell*.

O passo final foi executado via linha de comando do *PowerShell* (Figuras 1 e 2). Após esse passo, todos os usuários da plataforma Microsoft 365 passaram a ser redirecionados para a tela de login da plataforma da Google, confirmando o funcionamento correto da conexão federada entre as duas plataformas.

```
Na linha de comando do Powershell, digite os comandos:

# instalar módulo MsOnline
PS C:\Windows\System32> Install-Module MsOnline

# importar módulo MsOnline
PS C:\Windows\System32> Import-Module MSOnline

# conectar ao Microsoft 365 (com usuário administrador da plataforma)
PS C:\Windows\System32> Connect-MsolService

# armazenar em variável o domínio a ser configurado
PS C:\Windows\System32> $domainname = "unifal-mg.edu.br"

# verificar se o domínio está federado (caso negativo não haverá resposta do comando)
PS C:\Windows\System32> Get-MsolDomainFederationSettings -DomainName $domainname

# listar dos domínios da plataforma Microsoft 365
PS C:\Windows\System32> Get-MsolDomain

Name                                    Status     Authentication
----                                    ------     --------------
discentes.unifal-mg.edu.br              Verified   Managed
unifalmgedubr.onmicrosoft.com           Verified   Managed
unifal-mg.edu.br                        Verified   Managed
sou.unifal-mg.edu.br                    Verified   Managed
discentesunifalmgedubr.onmicrosoft.com Unverified Managed

# armazenar em variável os dados do IdP baixados da plataforma Google Workspace
PS C:\Windows\System32> [xml]$idp = Get-Content 'C:\Users\nti\Downloads\GoogleIdPMetadata.xml'

# mostrar os dados da entidade
PS C:\Windows\System32> $idp

xml                          EntityDescriptor
---                          ----------------
version="1.0" encoding="UTF-8" EntityDescriptor
```

Figura 1. Execução no PowerShell

```
# armazenar em variável o certificado do IdP (Google Workspace)
PS C:\Windows\System32> $signingCertificate =
  ($idp.EntityDescriptor.IDPSSODescriptor.KeyDescriptor.KeyInfo.X509Data.X509Certificate | Out-String).Trim()

# armazenar em variável a URL de login da plataforma Microsoft 365
PS C:\Windows\System32> $activeLogonUri = "https://login.microsoftonline.com/login.srf"

# armazenar em variável a URL do emissor (ID do Google Workspace)
PS C:\Windows\System32> $issuerUri = $idp.EntityDescriptor.entityID

# armazenar em variáveis as URLs de logon e logoff do IdP (Google Workspace)
PS C:\Windows\System32> $passiveLogOnUri = $idp.EntityDescriptor.IDPSSODescriptor.SingleSignOnService.Location[0]
PS C:\Windows\System32> $logOffUri = $idp.EntityDescriptor.IDPSSODescriptor.SingleSignOnService.Location[0]

# armazenar em variável um nome para a Federação
PS C:\Windows\System32> $federationbrandname = "Login Institucional UNIFAL-MG"

# configurar a federação no domínio com as variáveis criadas
PS C:\Windows\System32> Set-MsolDomainAuthentication -DomainName $domainname -FederationBrandName \
$federationbrandname -Authentication Federated -PassiveLogOnUri $passiveLogOnUri -ActiveLogOnUri $activeLogonUri \
-SigningCertificate $signingcertificate -IssuerUri $issuerUri -LogOffUri $logOffUri \
-PreferredAuthenticationProtocol "SAMLP"

# verificar se o resultado foi positivo
PS C:\Windows\System32> Get-MsolDomainFederationSettings -domainname $domainname


ActiveLogOnUri                        : https://login.microsoftonline.com/login.srf
DefaultInteractiveAuthenticationMethod :
FederationBrandName                   : Login Institucional UNIFAL-MG
IssuerUri                             : https://accounts.google.com/o/saml2?idpid=XxXxXxXxX
LogOffUri                             : https://accounts.google.com/o/saml2/idp?idpid=XxXxXxXxX
MetadataExchangeUri                   :
NextSigningCertificate                :
OpenIdConnectDiscoveryEndpoint        :
PassiveLogOnUri                       : https://accounts.google.com/o/saml2/ldp?ldpid=XxXxXxXxX
SigningCertificate                    : MIIDdDCCAlygAwIBAgIGAYZRJ1MxMA0GCSqGSIb3DQEBCwUAMHsxFDASBgNVBAoTC0dvb2dsZSBJ
                                        ..........
                                        MqlrdUZZOtkWDyv7B+uDFroFgggtPKh6ZIC+5Tm/SWSNG0IA5SMGf4tcyxyL1YGbfJr4OS30OYkf
                                        mErXpdDmzDeEzppLvqOE219sXt2DAATi0MkBnZ7YKNjN
SupportsMfa                           :

# voltar a configuração do domínio para gerenciado ao invés de federado (caso necessário)
PS C:\Windows\System32> Set-MsolDomainAuthentication -DomainName $domainname -Authentication managed
```

Figura 2. Execução no PowerShell (continuação)

A execução do *script PowerShell*, além de configurar as licenças para cada usuário, executa outras configurações nas contas, necessárias para o licenciamento correto e desativa ferramentas desnecessárias da plataforma. O *script* é executado semanalmente e atribui, primeiramente, a localização “BR” para todos os usuários, para que as licenças sejam atribuídas de acordo com as oferecidas no Brasil. Para os usuários do domínio unifal-mg.edu.br são atribuídas as licenças STANDARDWOFFPACK_FACULTY, POWER_BI_STANDARD, FLOW_FREE e POWERAPPS_DEV. Para os usuários do subdomínio colab.unifal-mg.edu.br é atribuída a licença STANDARDWOFFPACK_FACULTY. Para os usuários do subdomínio sou.unifal-mg.edu.br são atribuídas as licenças STANDARDWOFFPACK_STUDENT e POWER_BI_STANDARD. Em todas as licenças do tipo STANDARDWOFFPACK o plano de serviço EXCHANGE_S_STANDARD (Outlook) é desativado para não entrar em conflito com o e-mail que é oferecido pela plataforma da Google.

Essa metodologia proporcionou uma implementação eficiente e otimizada, garantindo uma experiência simples para a comunidade acadêmica da UNIFAL-MG.

Resultados e discussão

A implementação da conexão federada entre a plataforma Google Workspace e a plataforma Microsoft 365 e a configuração automatizada de licenças por meio do *script PowerShell* desenvolvido, demonstrou resultados significativos na gestão e licenciamento de usuários. Esse processo foi fundamental para que a comunidade acadêmica da UNIFAL-MG pudesse aproveitar plenamente os aplicativos e licenças disponibilizados pela plataforma da Microsoft.

Principais resultados obtidos com a implementação:

- gestão centralizada e automatizada de usuários;
- licenciamento automatizado de acordo com o perfil de cada usuário;
- licenciamento automatizado de toda a comunidade acadêmica;
- licenciamento apenas de usuários autorizados;
- ampliação da utilização das ferramentas disponíveis;

- opção de escolha pelo conjunto de ferramentas que o usuário mais se adapta;
- utilização de login único para conexão;
- pouco suporte técnico dispendido na implantação, devido a utilização de plataformas consolidadas;
- suporte técnico oficial do NTI;
- nenhuma alteração em sistemas internos, já adequados para a plataforma Google Workspace;
- adequação às normativas internas.

Conclusões

A utilização da conexão federada entre a plataforma Google Workspace e a plataforma Microsoft 365 revelou-se uma iniciativa estratégica e bem-sucedida na UNIFAL-MG. A adoção do provisionamento automático de usuários, o login único e a configuração automatizada de licenças representaram avanços cruciais para proporcionar à comunidade acadêmica uma experiência mais eficiente e acessível à plataforma da Microsoft. A utilização das licenças gratuitas para discentes e docentes disponíveis na plataforma da Microsoft aprimorou os processos de ensino, pesquisa e extensão ampliando o acesso às ferramentas da plataforma pela comunidade. O comprometimento do NTI em buscar soluções inovadoras demonstra o papel vital da tecnologia da informação na promoção do sucesso acadêmico e na adaptação às demandas contemporâneas. O sucesso da solução destaca-se como um exemplo inspirador para outras instituições de ensino que buscam disponibilizar, cada vez mais, ferramentas para beneficiar plenamente sua comunidade acadêmica.

Referências

Goldy Arora. **Google Workspace to Office 365 SSO and Provisioning Guide**. Disponível em: <https://www.goldyarora.com/blog/g-suite-to-office-365-sso>. Acesso em abr. 2023.

Google. **Configurar o provisionamento automático do Microsoft Office 365**. Disponível em: <https://support.google.com/a/answer/7365072>. Acesso em abr. 2023.

Google. **Configurar o SSO via SAML para o Microsoft Office 365**. Disponível em: <https://support.google.com/a/answer/6363817?hl=pt-BR>. Acesso em abr. 2023.

Microsoft. **Configurar a federação entre o Google Workspace e Microsoft 365**. Disponível em: <https://learn.microsoft.com/pt-br/education/windows/configure-aad-google-trust>. Acesso em abr. 2023.

Microsoft. **Microsoft Graph PowerShell documentation**. Disponível em: <https://learn.microsoft.com/en-us/powershell/microsoftgraph/?view=graph-powershell-1.0>. Acesso em abr. 2023.

Microsoft. **O que é o PowerShell**. Disponível em: <https://learn.microsoft.com/pt-br/powershell/scripting/overview?view=powershell-7.4>. Acesso em abr. 2023.