

Protegendo contas privilegiadas com ferramentas *open source*

TLP:CLEAR

PALESTRANTE

ANDRÉ TORRES



WHOAMI

- ✓ Auditor de cibersegurança (2010)
 - ✓ APF – crimes cibernéticos (2005-2010)
- ✓ Bacharel em Ciência da Computação pela Universidade de Brasília (UnB). Pós-graduado em Segurança da Informação (UPIS) e em Governança de Tecnologia da Informação e Comunicação no Setor Público (UnB).
- ✓ Experiência nas áreas de gestão de incidentes e vulnerabilidades, segurança em infraestrutura do AD, ofensiva e auditoria.
- ✓ Consultor de cibersegurança e instrutor de cursos de AD, ADCS, Purple Team

andretorresbr



O desafio da gestão de acesso privilegiado



Atacante não mais
hackeia, ele **acessa**

79% dos ataques de ransomware usaram identidades como vetor de
acesso inicial

Descoberta foi documentada no State of Ransomware 2026 da Sophos, anunciada hoje (15) pela empresa. De acordo com os executivos da companhia, esse cenário é fruto de uma coordenação maior de diversos eventos maliciosos a partir da Inteligência Artificial, exigindo que a Cibersegurança caminhe com mais urgência à defesa interconectada

Por: Matheus Bracco | julho 15, 2026 | Destaques

O desafio da gestão de acesso privilegiado

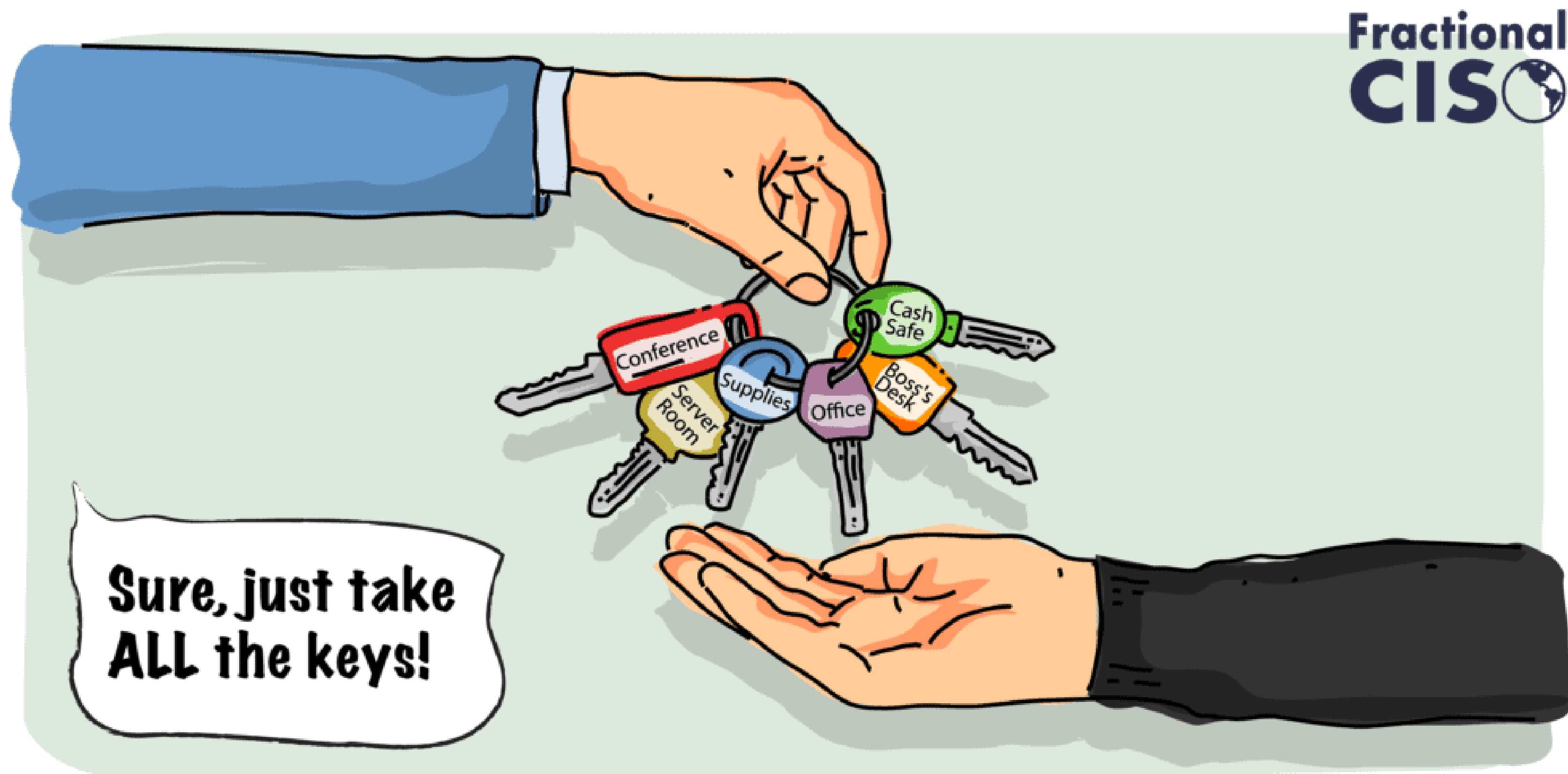
- Dificuldades da gestão de contas privilegiadas
- Senhas fracas

Login: admin
Password: admin



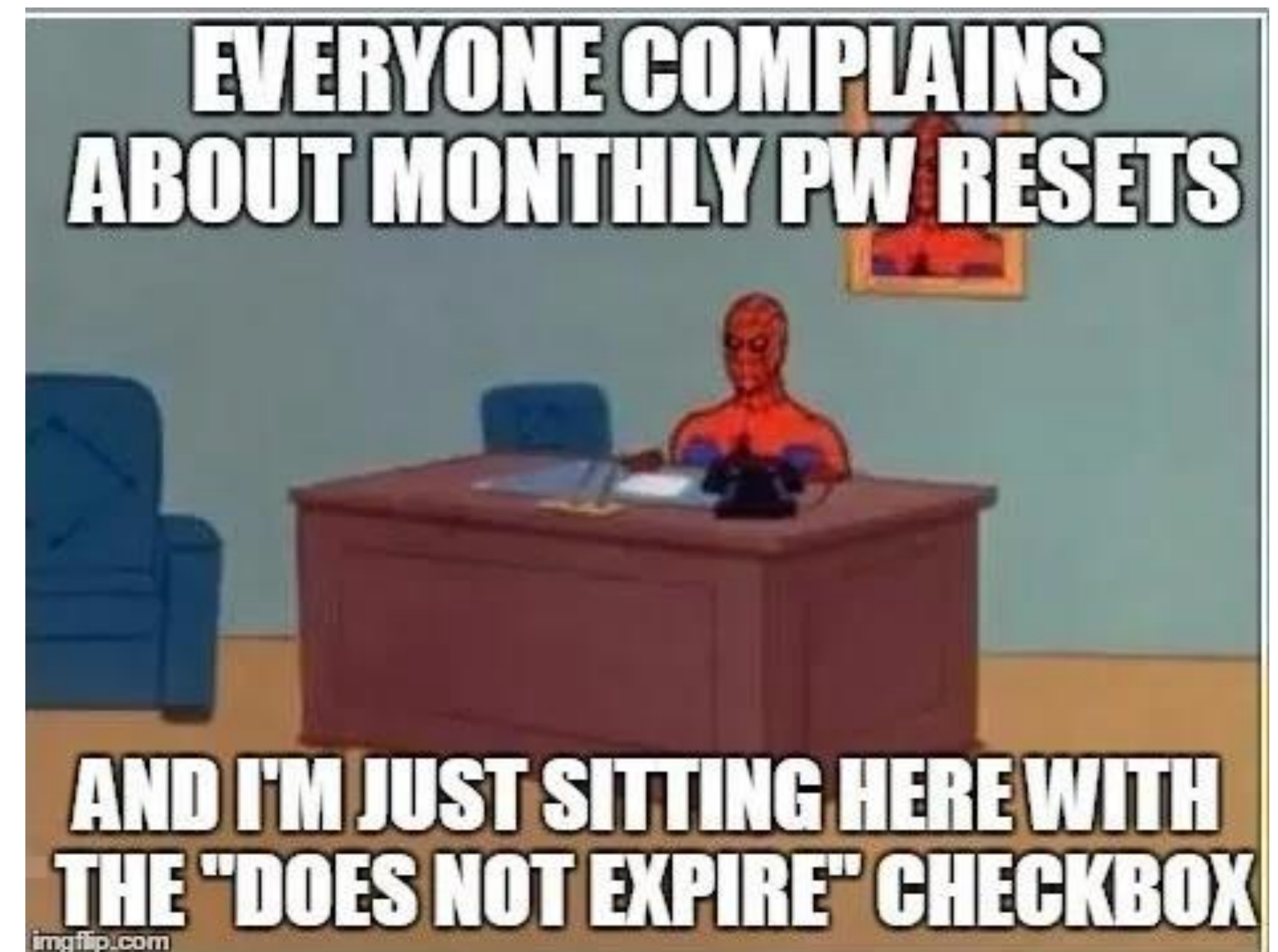
O desafio da gestão de acesso privilegiado

- Dificuldades da gestão de contas privilegiadas
 - Excesso de privilégios + privilégios constantes



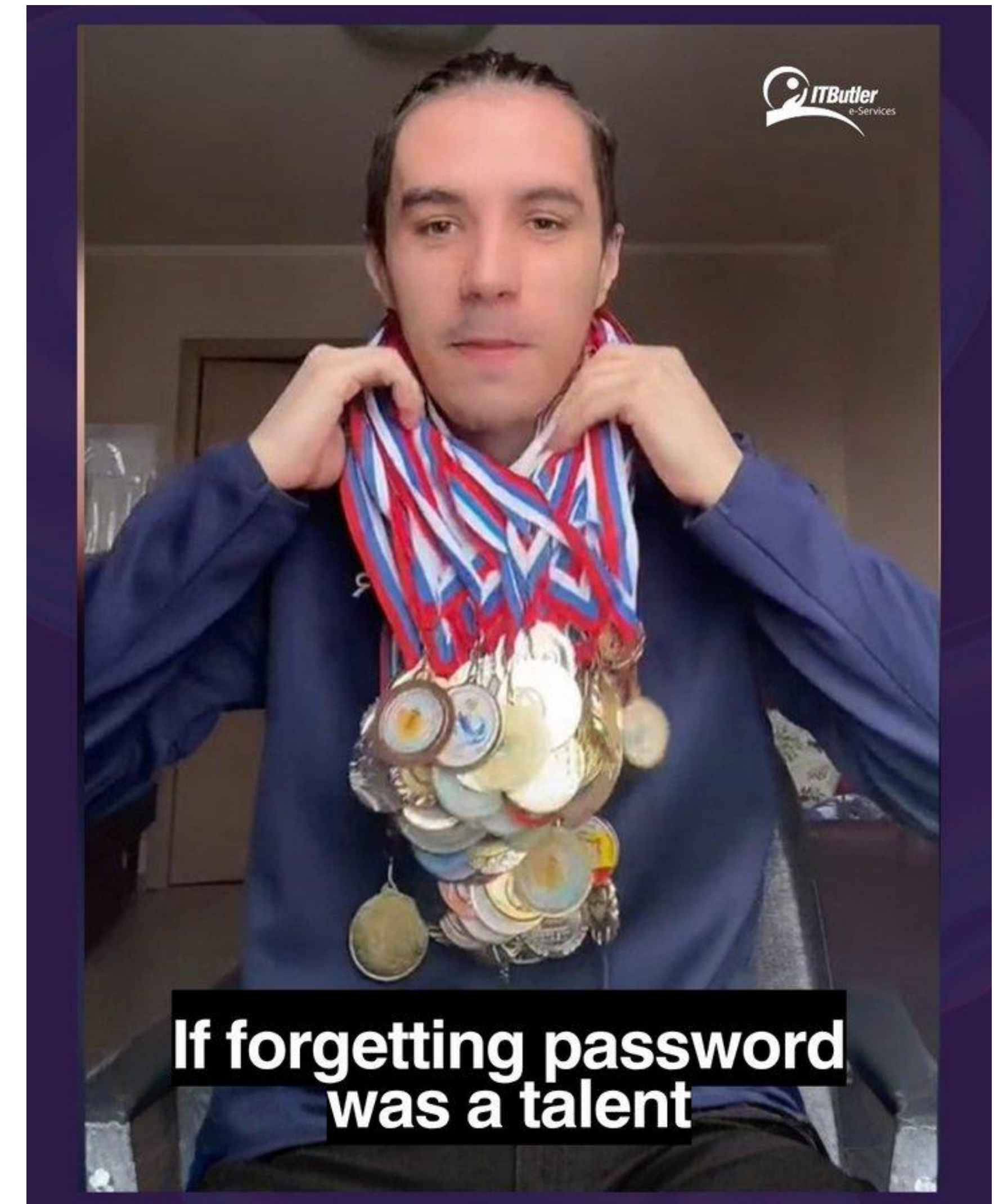
O desafio da gestão de acesso privilegiado

- Dificuldades da gestão de contas privilegiadas
 - Senhas imutáveis, sequenciais ou raramente modificadas

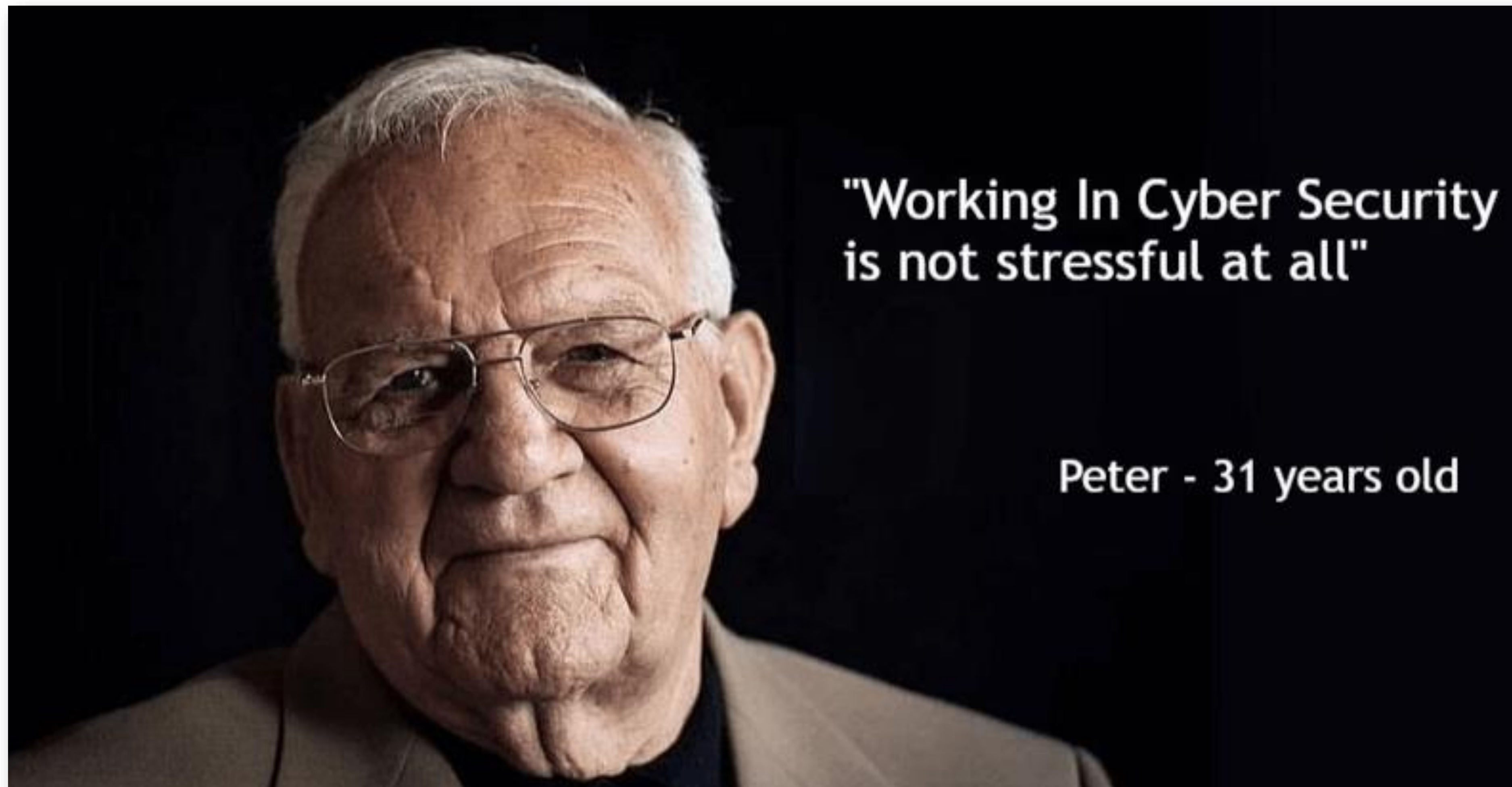


O desafio da gestão de acesso privilegiado

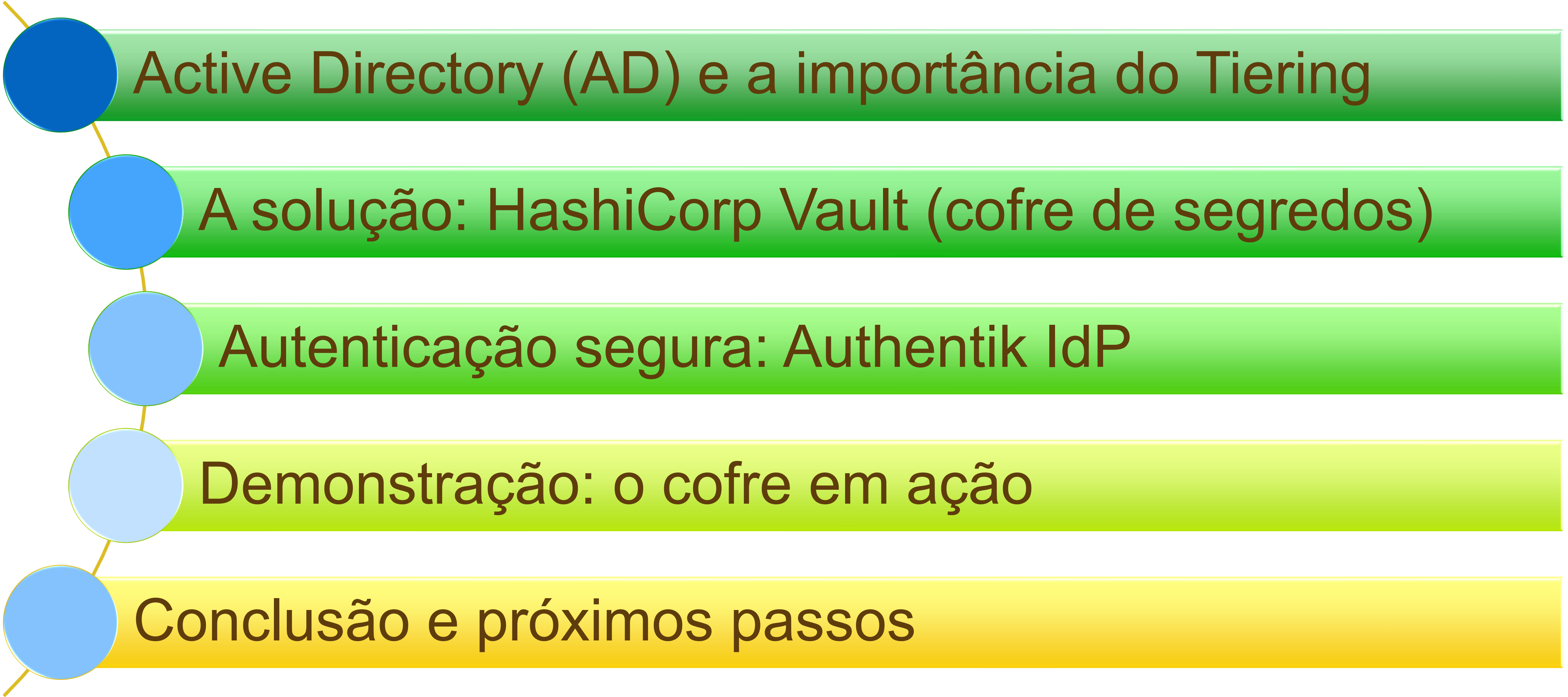
- Dificuldades da gestão de contas privilegiadas
 - **Se não for fraca, onde armazená-las?**
- Na vida **peessoal**, usamos gerenciadores de senhas
 - Bitwarden, LastPass, 1Password, etc
- E na vida **corporativa**?



O desafio da gestão de acesso privilegiado



Agenda



Active Directory (AD) e a importância do Tiering

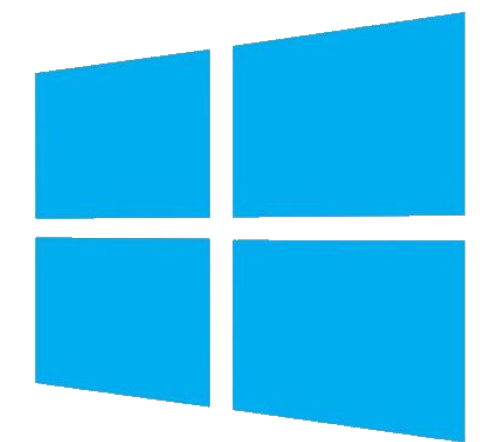
A solução: HashiCorp Vault (cofre de segredos)

Autenticação segura: Authentik IdP

Demonstração: o cofre em ação

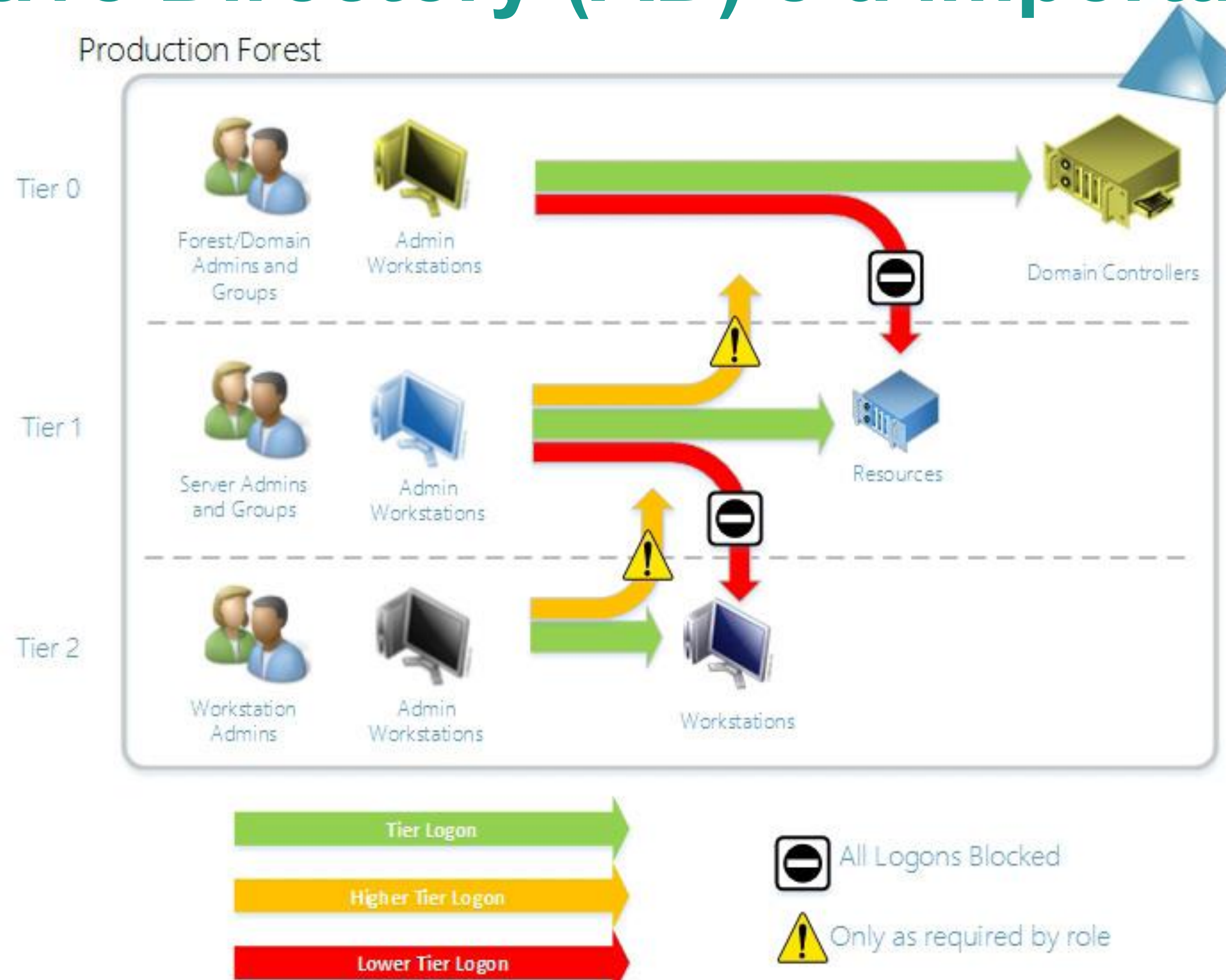
Conclusão e próximos passos

Active Directory (AD) e a importância do Tiering



Active Directory

Active Directory (AD) e a importância do Tiering



andre.torres_da

andre.torres_a

andre.torres

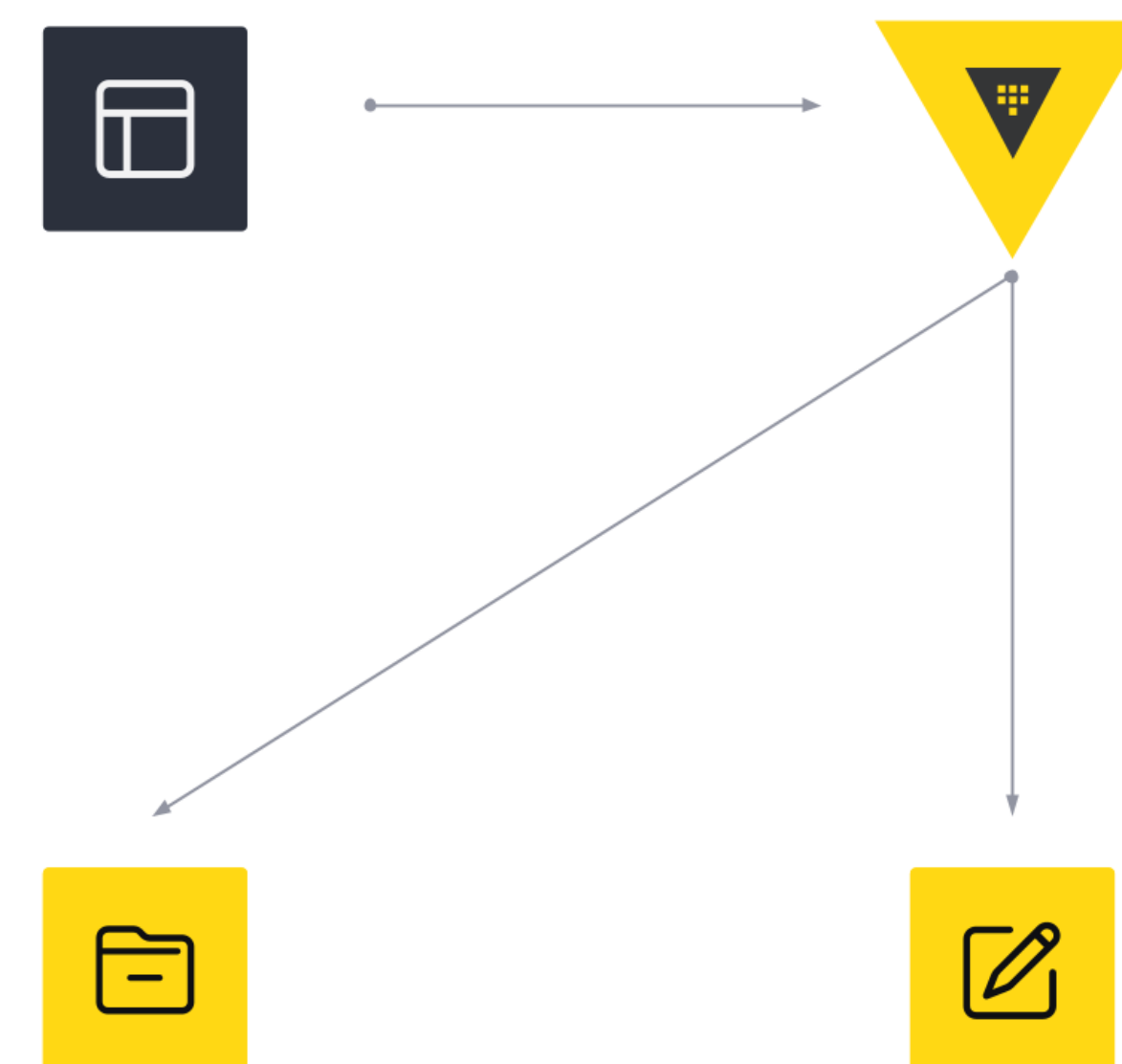
A solução: HashiCorp Vault (cofre de segredos)

- Ferramenta aberta para gerenciamento e acesso a **secrets**
 - 2023 mudou licença para BSL, fork *OpenBao*
 - Armazena chaves de API, usuários + senhas, certificados, tokens, etc
- Provê interface de acesso unificada aos secrets
 - Controle de acesso: quem pode acessar uma secret
 - Logs de auditoria detalhado: quem acessou o que
- Centralização de secrets que antes estavam espalhados em estações de devs e servidores (*secret sprawl*)



A solução: HashiCorp Vault (cofre de segredos)

- Gerenciamento de secrets
- **Estáticos** (“*KeePass corporativo com API*”)
 - Armazena secrets no cofre de forma criptografada
 - Não expiram ou revogam a credencial
 - Credenciais permanentes
 - Ex: credencial de um usuário permanente no SGBD
- **Dinâmicos** (JIT)
 - Criação de secrets no momento e com vida curta
 - Credenciais temporárias (TTL)
 - Ex: credencial temporária de SGBD para uma operação específica



A solução: HashiCorp Vault (cofre de segredos)

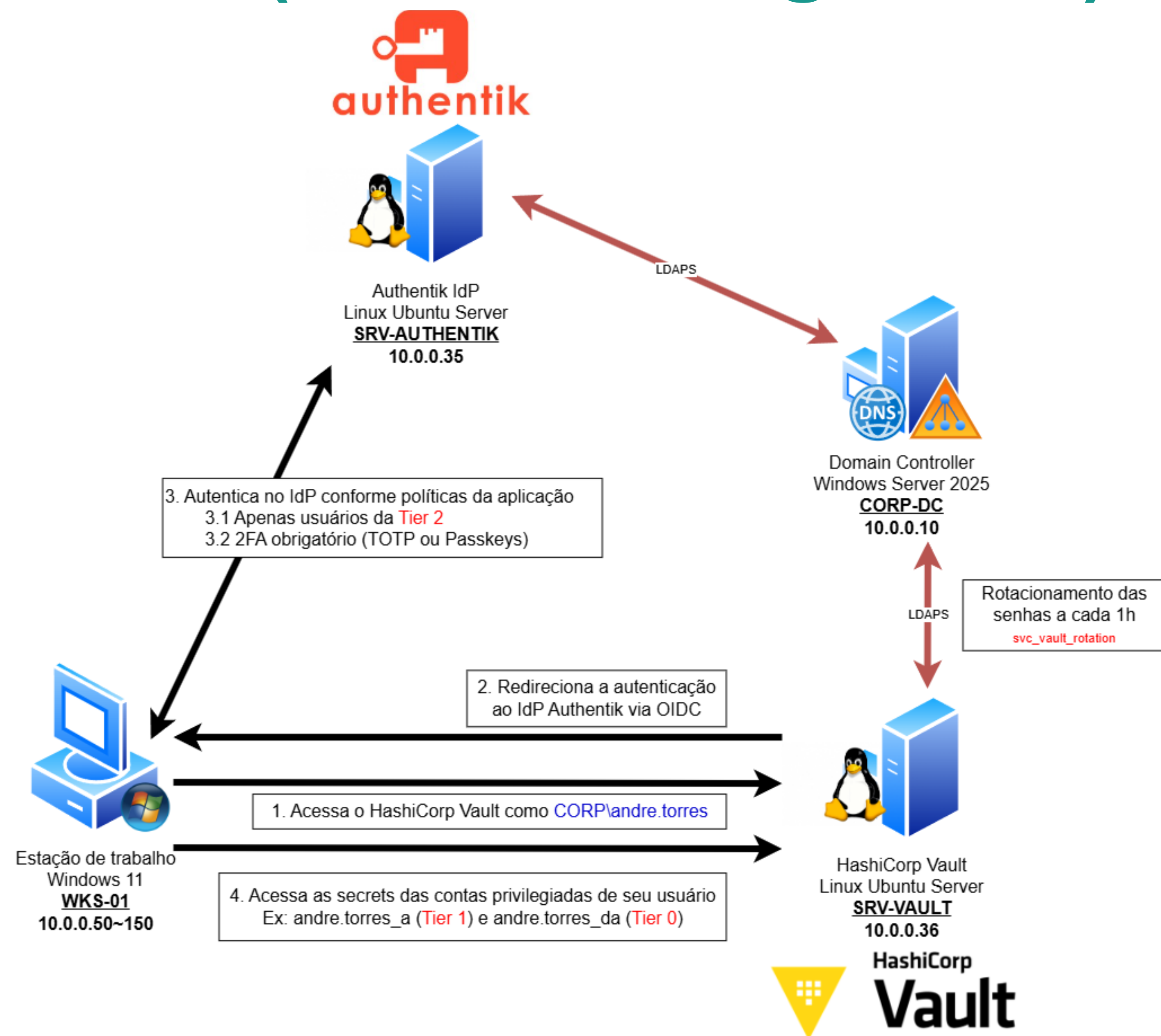
- Secrets engines
 - Plugins de gerenciamento de soluções
 - Banco de dados (PostgreSQL, MySQL, MongoDB, MSSQL, Oracle, Snowflake, etc)
 - Plataformas Cloud (AWS, Azure, GCP)
 - Orquestração (Kubernetes, Nomad)
 - Redes e acesso (Consul, RabbitMQ, SSH)
- TOTP
- PKI
- LDAP/S



HashiCorp
Vault

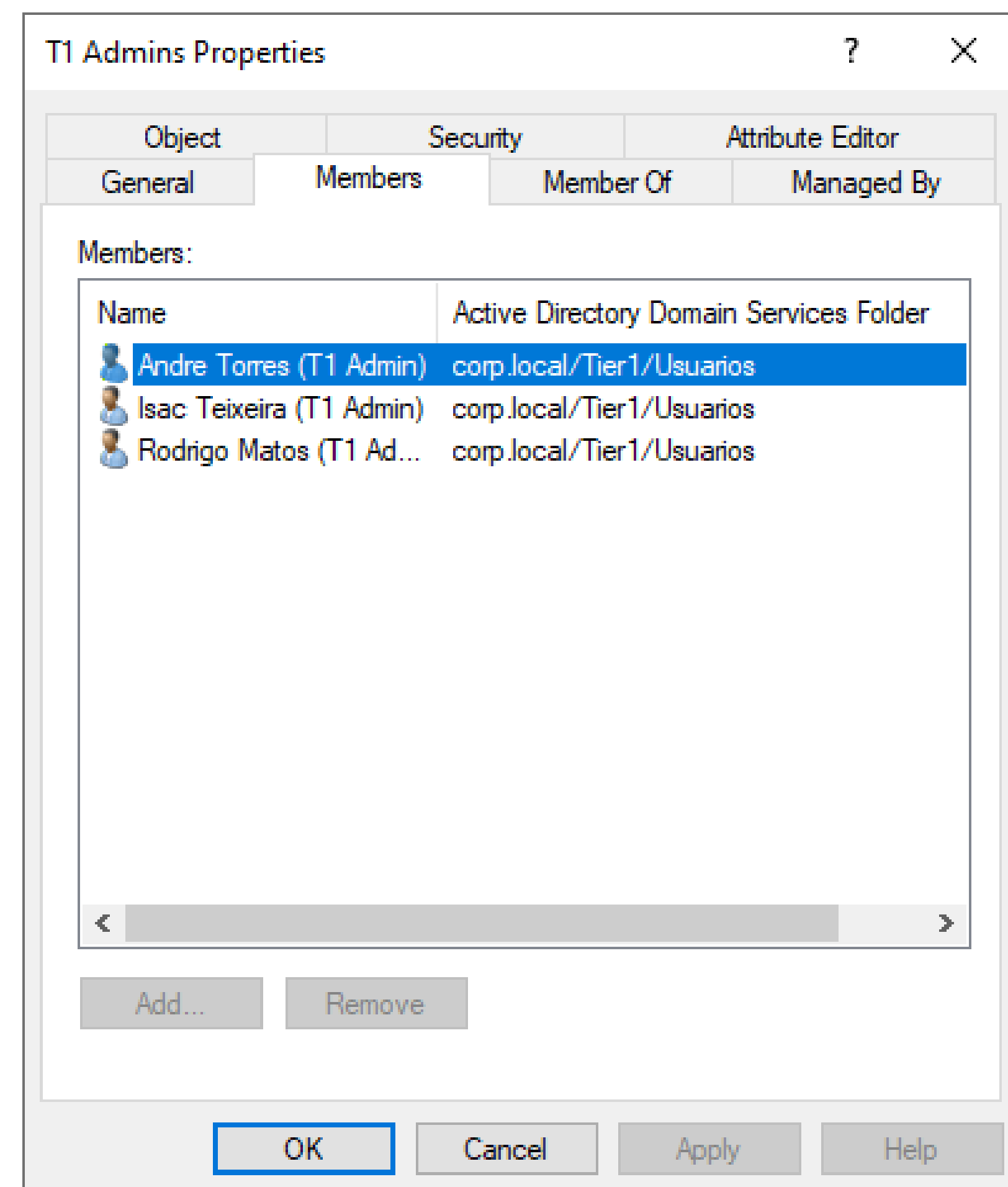
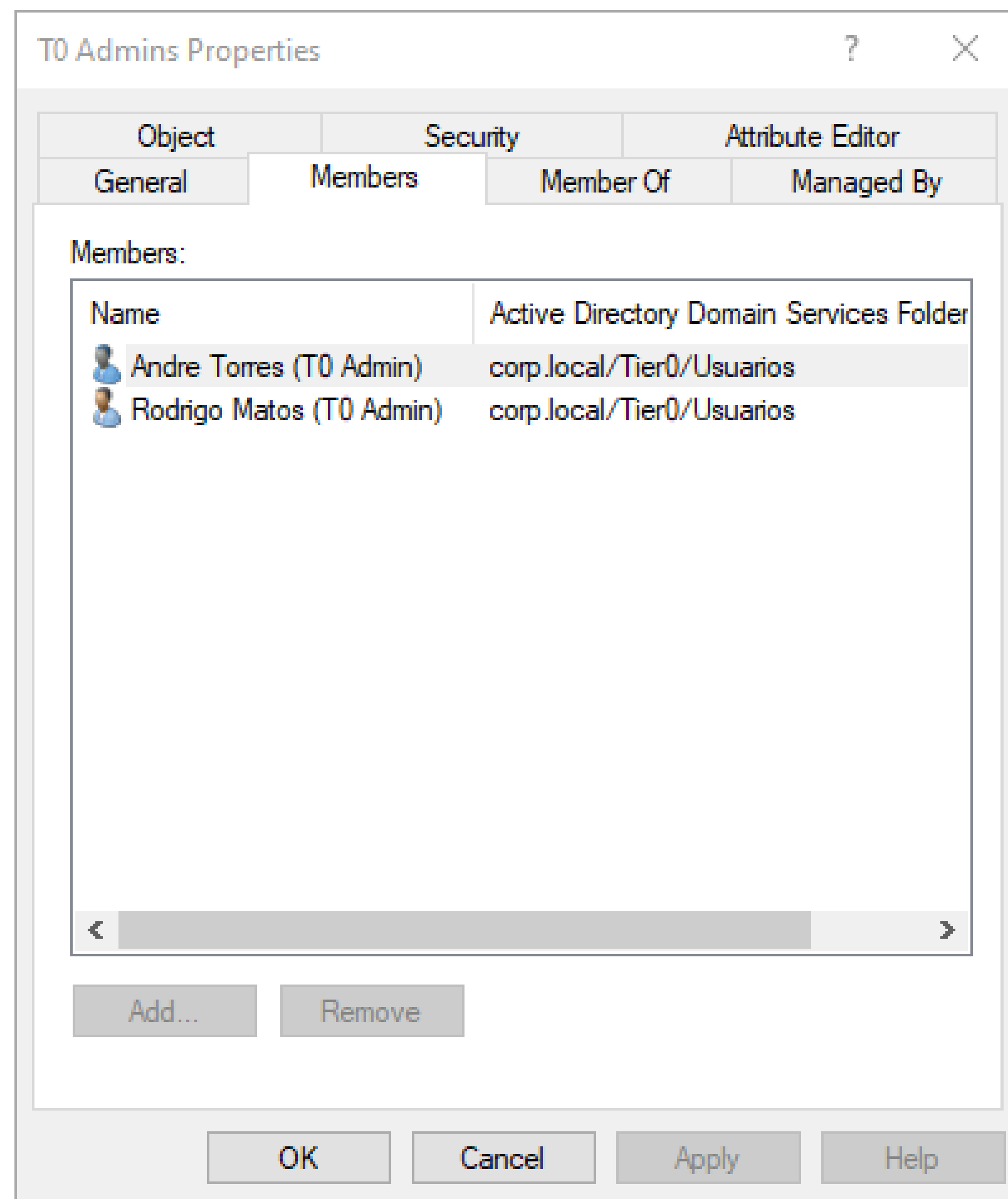
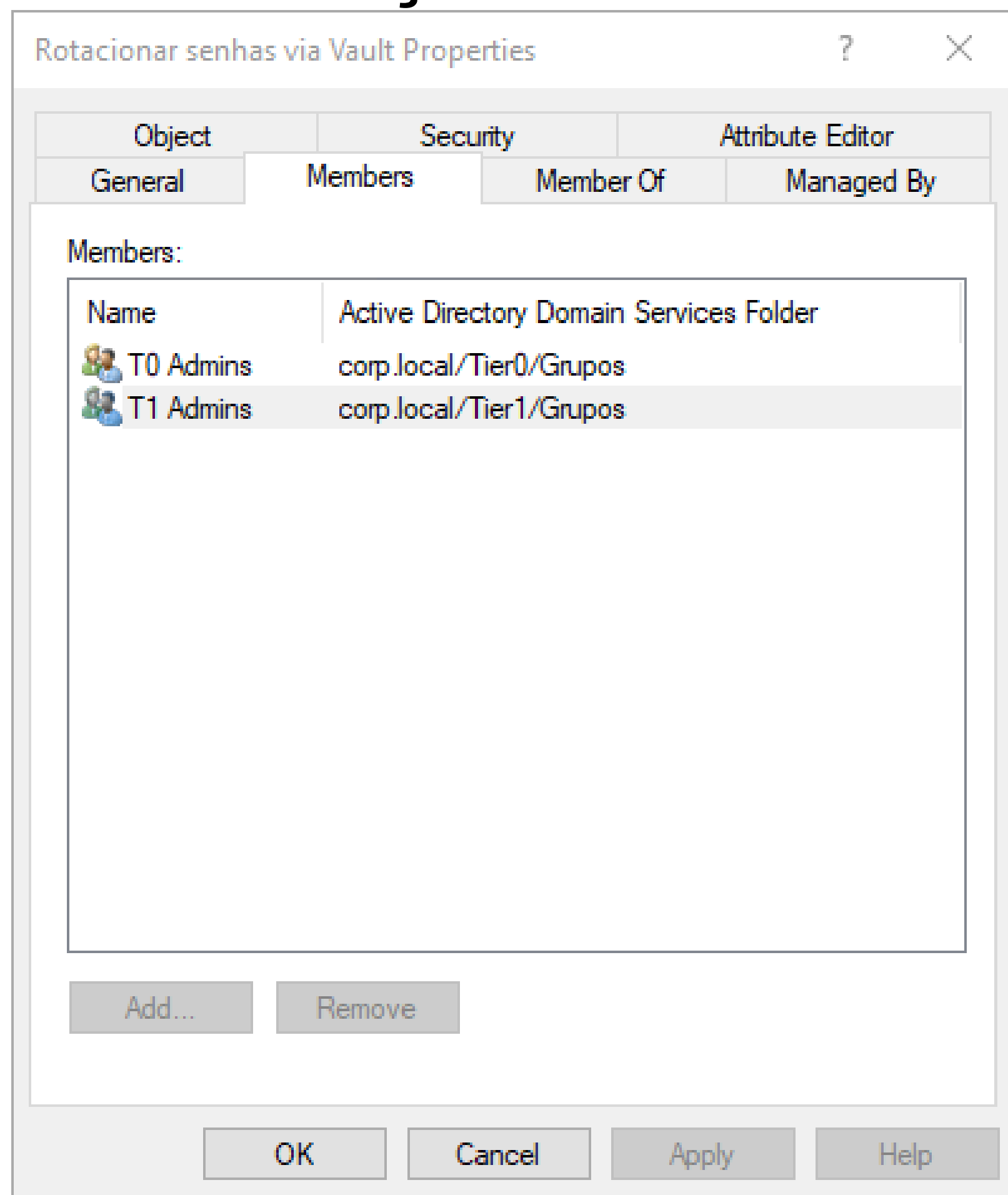
A solução: HashiCorp Vault (cofre de segredos)

- Secrets engine escolhida: **LDAP/S**
- Rotação das senhas de contas privilegiadas (Tier 0 e Tier 1) a cada 1h
- Senhas complexas de 64 caracteres
- Usuário **username** só tem acesso à senha de suas contas **username_a** e **username_da** via Vault



A solução: HashiCorp Vault (cofre de segredos)

- Para um usuário ter sua senha rotacionada, basta incluí-lo no grupo de rotação de senhas



A solução: HashiCorp Vault (cofre de segredos)

- Script de sincronismo
 - Executa a cada 6hs
 - Varre os membros do grupo do AD e garante que todos estão sendo gerenciados pelo Vault
 - Se algum usuário foi inserido no grupo, insere no Vault
 - Se algum usuário foi removido do grupo, remove do Vault

```
root@srv-vault:/opt/vault/sync# vault list corp.local/static-role/  
Keys  
----  
andre.torres_a  
andre.torres_da  
isac.teixeira_a  
rodrigo.matos_a  
rodrigo.matos_da  
root@srv-vault:/opt/vault/sync#
```


A solução: HashiCorp Vault (cofre de segredos)

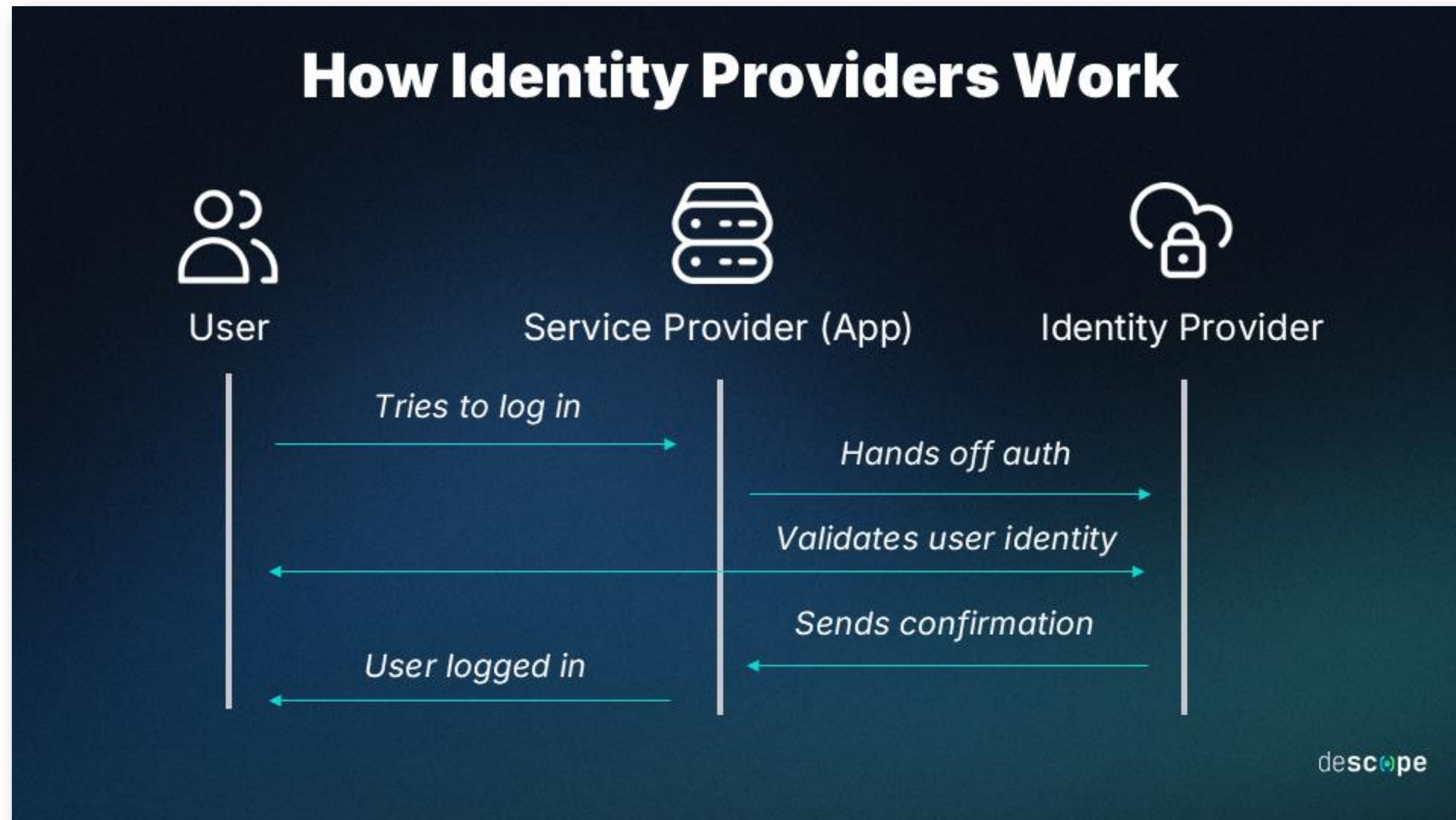
- Script de sincronismo

```
root@srv-vault:/opt/vault/sync# cat logs/2026/06/2026-06-10.log

=====
--- INÍCIO DA SINCRONIZAÇÃO AD/VAULT (Wed Jun 10 18:00:01 -03 2026) ---
=====
--- Autenticando no Vault via AppRole ---
[SUCESSO] Autenticado e token de curta duração obtido.
Buscando contas de serviço recursivamente no grupo 'Rotacionar senhas via Vault' (DN: CN=Rotacionar senhas via Vault,OU=Papeis,OU=Tier0,DC=corp,DC=local)...
Contas de Serviço encontradas para Static Roles:
andre.torres_a
isac.teixeira_a
rodrigo.matos_a
andre.torres_da
rodrigo.matos_da
--- Processando criação de Static Roles ---
-> Processando role: andre.torres_a
[INFO] Static role andre.torres_a já existe. Pulando criação.
-> Processando role: isac.teixeira_a
[INFO] Static role isac.teixeira_a já existe. Pulando criação.
-> Processando role: rodrigo.matos_a
[INFO] Static role rodrigo.matos_a já existe. Pulando criação.
-> Processando role: andre.torres_da
[INFO] Static role andre.torres_da já existe. Pulando criação.
-> Processando role: rodrigo.matos_da
[INFO] Static role rodrigo.matos_da já existe. Pulando criação.
--- Processando limpeza de Static Roles obsoletas ---
=====
--- FIM DA SINCRONIZAÇÃO AD/VAULT (Wed Jun 10 18:00:02 -03 2026) ---
=====
--- Revogando token AppRole ---
root@srv-vault:/opt/vault/sync#
```

A solução: HashiCorp Vault (cofre de segredos)

- Como proteger o acesso ao Vault?
- Autenticação OAuth2/OIDC com Identity Provider (IdP) - MFA seguro



Fonte: <https://www.descope.com/learn/post/identity-provider>

Autenticação segura: Authentik IdP

- Soluções abertas de IdP: Keycloak, Authelia, Authentik



Welcome to authentik!

Email or Username *

Log in

Or

Use a security key



[Forgot username or password?](#)

Core Capabilities	authentik	Okta	Microsoft ADFS	Azure/Entra ID	Keycloak	Duo	Authelia
Self-host Anywhere	✓	✗	⚠	✗	✓	✗	✓
MFA ⓘ	✓	✓	✗	✓	✓	✓	✓
Conditional Access	✓	✓	✓	⚠	✓	⚠	✓
Open-source/Source Available	✓	✗	✗	✗	✓	✗	✓
Application Proxy	✓	✗	⚠	✓	⚠	✗	✗
FIPS Compliance	✓	⚠	✓	✓	✓	⚠	✗
Enterprise Support	✓	✓	✗	✓	⚠	✓	✗
WebAuthn (Passkeys)	✓	✓	✓	✓	✓	✓	✓
GeoIP / Impossible Travel	✓	✓	✓	✓	✗	✓	✗
Remote Access (RDP, VNC, SSH)	✓	✗	✗	✗	✗	✗	✗
OIDC Back-Channel Logout	✓	✗	✗	✗	✓	✗	✗

Autenticação segura: Authentik IdP

- Autenticação LDAPs integrada ao Active Directory



Connection settings

Server URI *

ldaps://corp-dc.corp.local:636

Specify multiple server URIs by separating them with a comma.



Enable StartTLS

To use SSL instead, use 'ldaps://' and disable this option.



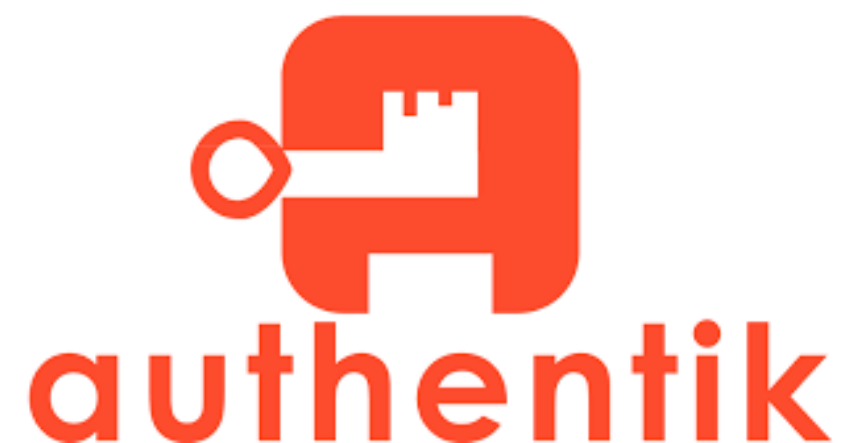
Use Server URI for SNI verification

Required for servers using TLS 1.3+

TLS Verification
Certificate

rootca

When connecting to an LDAP Server with TLS, certificates are not checked by default. Specify a keypair to validate the remote certificate.



Autenticação segura: Authentik IdP

- Enforcement de MFA para todos os usuários

Stage used to validate any authenticator. This stage should be used during authentication or authorization flows.

Name *

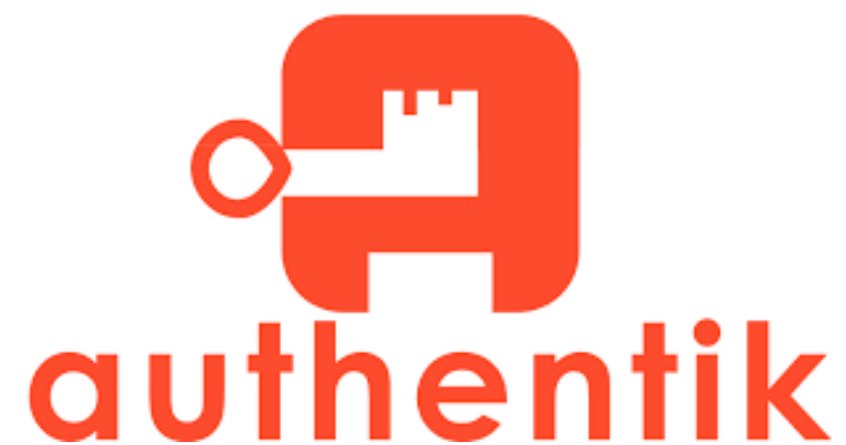
default-authentication-mfa-validation

▼ Stage-specific settings

Device classes *

- ☐ Static Tokens
- ☒ TOTP Authenticators
- ☒ WebAuthn Authenticators
- ☐ Duo Authenticators
- ☐ SMS-based Authenticators
- ☐ Email-based Authenticators

Device classes which can be used to authenticate.



Not configured
action *

Force the user to configure an authenticator



Autenticação segura: Authentik IdP

- Criação de Application e Provider OIDC no Authentik

New application
Create a new application and configure a provider for it.

1 Application

2 Choose a Provider

3 Configure Provider

4 Configure Bindings

5 Review and Submit Application

Configure The Application

Name * HashiCorp Vault
The name displayed in the application

Slug * hashi-corp-vault
Internal application name used in URL

Group e.g. Collaboration, Communication
Optionally enter a group name. Application will be created under this group.

Policy engine mode * ☒ ANY
Any policy must match to grant access

☐ ALL
All policies must match to grant access

> UI Settings

Next **Cancel**

New application
Create a new application and configure a provider for it.

1 Application

2 Choose a Provider

3 Configure Provider

4 Configure Bindings

5 Review and Submit Application

Choose a Provider Type

OAuth2/OpenID Provider
OAuth2 Provider for generic OAuth and OpenID Connect Applications.

SAML Provider
SAML 2.0 Endpoint for applications which support SAML.

RAC Provider
Remotely access computers/servers via RDP/SSH/VNC.

Proxy Provider
Protect applications that don't support any of the other Protocols by using a Reverse-Proxy.

Radius Provider
Allow applications

LDAP Provider
Allow applications

SCIM
SCIM 2.0 provider

Next **Back** **Cancel**

Autenticação segura: Authentik IdP

- Restrição via policy: apenas usuários Tier 2 se autenticam no Vault

New application

Create a new application and configure a provider for it.

1 Application

2 Choose a Provider

3 Configure Provider

4 **Configure Bindings**

5 Review and Submit Application

Configure Policy Bindings

These policies control which users can access this application.

Bind existing policy/group/user

Delete

☐	Order ↓	Binding
☐	-1	Policy Apenas usuarios da Tier 2

Executes the python snippet to determine whether to allow or deny a request.

Name * Apenas usuarios da Tier 2

☒ Execution logging
When this option is enabled, all executions of this policy will be logged. By default, only execution errors are logged.

Policy-specific settings

Expression *

```
1 # Verifica se o DN do usuário está dentro da OU desejada
2 user_dn = request.user.attributes.get("distinguishedName", "").lower()
3 return user_dn.endswith("ou=usuarios,ou=tier2,dc=corp,dc=local")
```

Expression using Python. [See documentation for a list of all variables.](#)

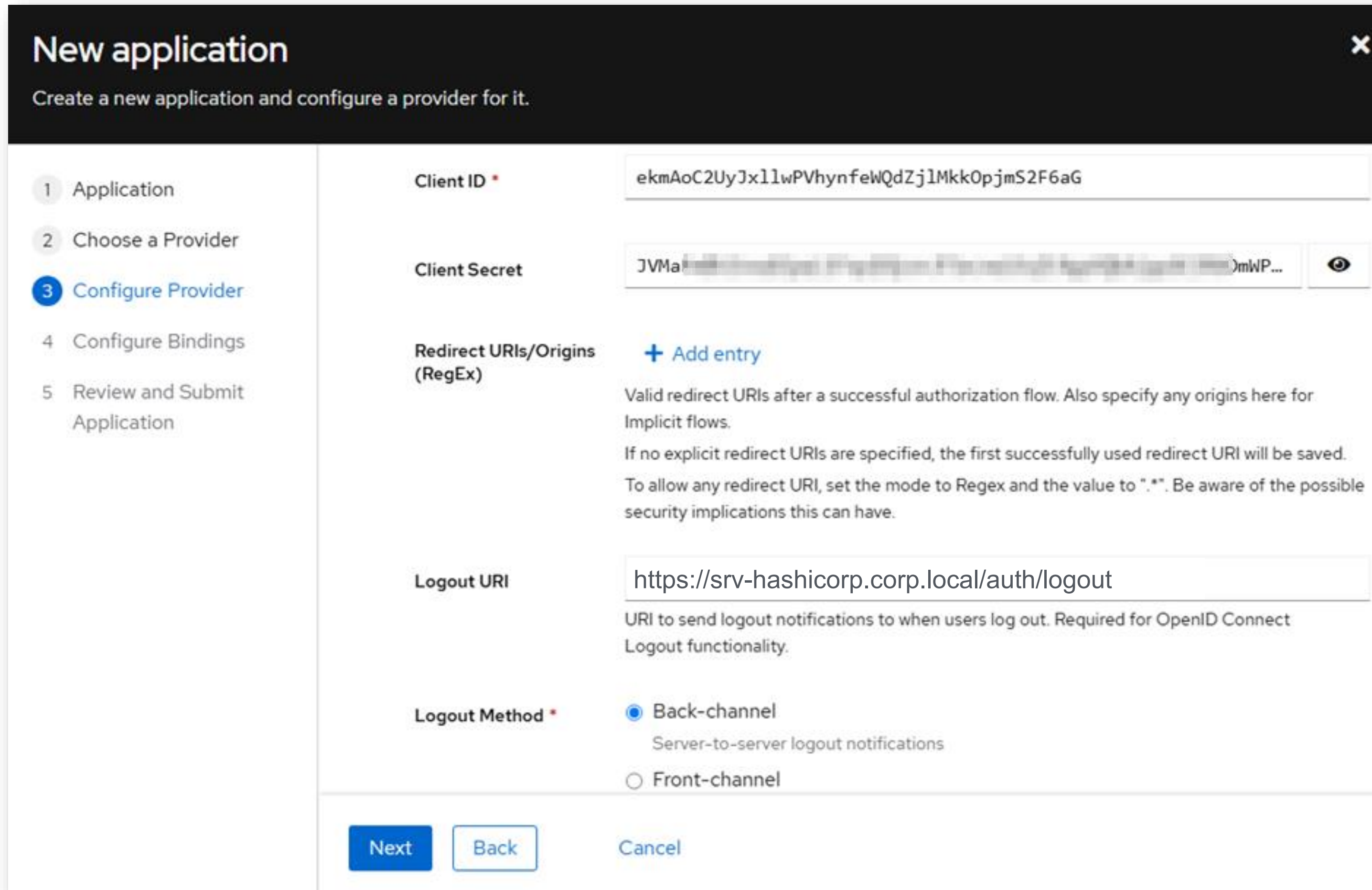
Next

Back

Cancel

Integração LAM + Authentik com 2FA

- Criação de Application e Provider OIDC no Authentik



The screenshot shows the 'New application' form in Authentik, specifically the 'Configure Provider' step. The form is titled 'New application' with a subtitle 'Create a new application and configure a provider for it.' The left sidebar shows a progress bar with five steps: 1. Application, 2. Choose a Provider, 3. Configure Provider (selected), 4. Configure Bindings, and 5. Review and Submit Application. The main form area contains the following fields:

- Client ID ***: ekmAoC2UyJx1lwPVhynfeWQdZjlMkkOpjmS2F6aG
- Client Secret**: JvMa... (masked) with an eye icon to toggle visibility.
- Redirect URIs/Origins (Regex)**: Includes a '+ Add entry' button and explanatory text: 'Valid redirect URIs after a successful authorization flow. Also specify any origins here for Implicit flows. If no explicit redirect URIs are specified, the first successfully used redirect URI will be saved. To allow any redirect URI, set the mode to Regex and the value to ".*". Be aware of the possible security implications this can have.'
- Logout URI**: https://srv-hashicorp.corp.local/auth/logout. Text below: 'URI to send logout notifications to when users log out. Required for OpenID Connect Logout functionality.'
- Logout Method ***: Radio buttons for 'Back-channel' (selected) and 'Front-channel'. Text below 'Back-channel': 'Server-to-server logout notifications'.

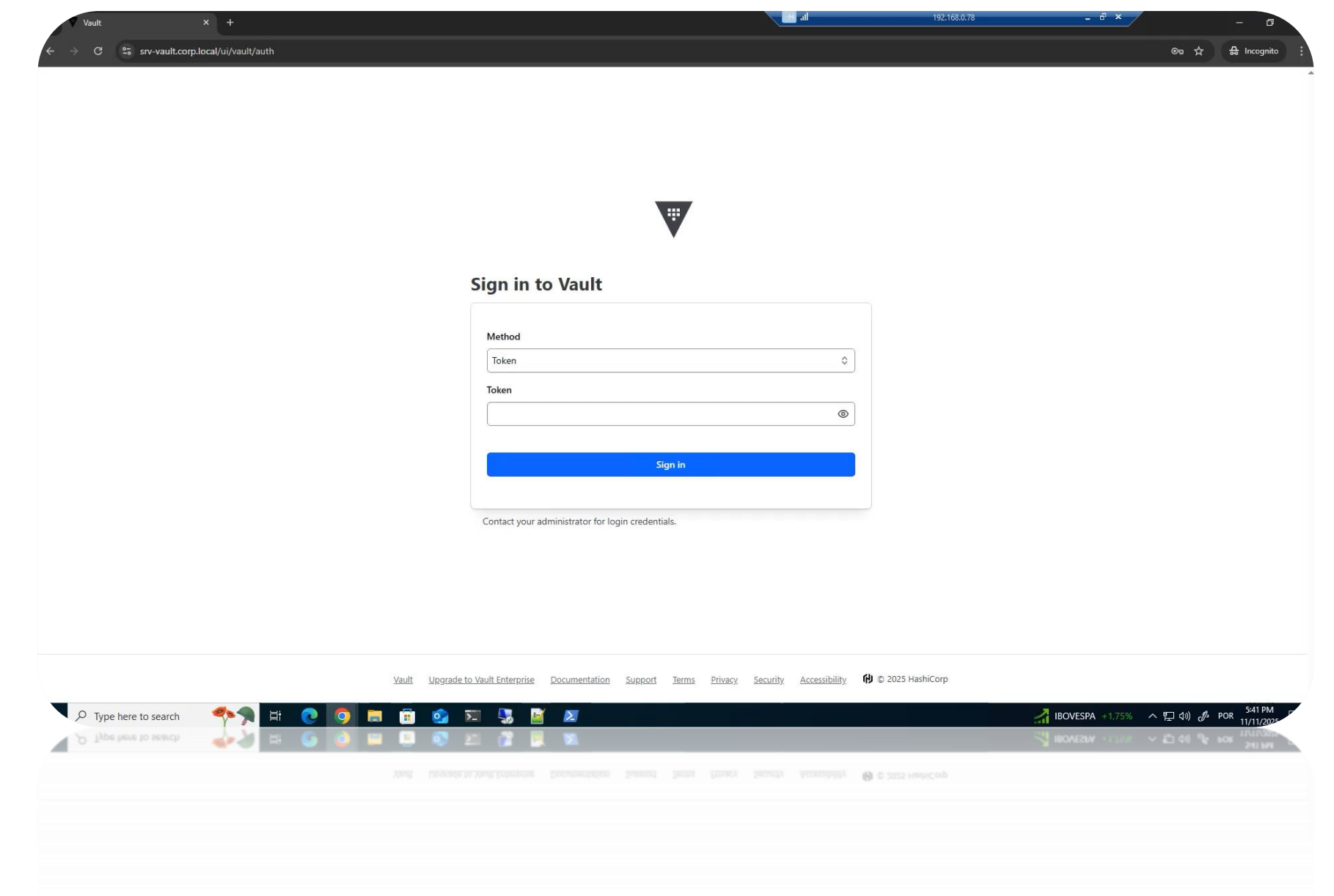
At the bottom, there are three buttons: 'Next' (blue), 'Back' (light blue), and 'Cancel' (light blue).

Subject mode *

- ☐ Based on the User's hashed ID
- ☐ Based on the User's ID
- ☐ Based on the User's UUID
- ☐ Based on the User's username
- ☐ Based on the User's Email
 - This is recommended over the UPN mode.
- ☒ Based on the User's UPN
 - Requires the user to have a 'upn' attribute set, and user ID. Use this mode only if you have different L
 - Configure what data should be used as unique

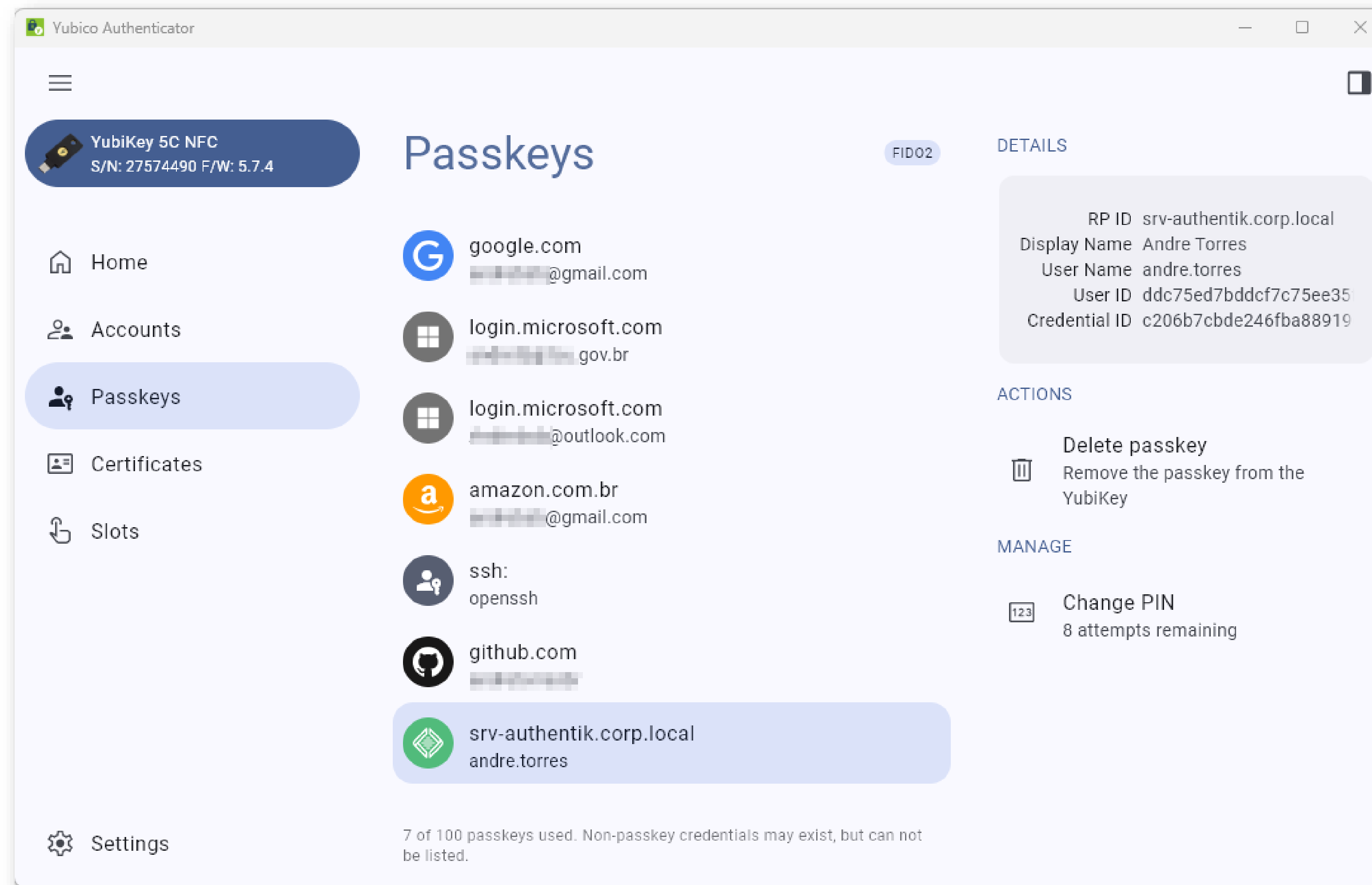
Demonstração: o cofre em ação

- Cenário: acesso válido às credenciais usando Passkey



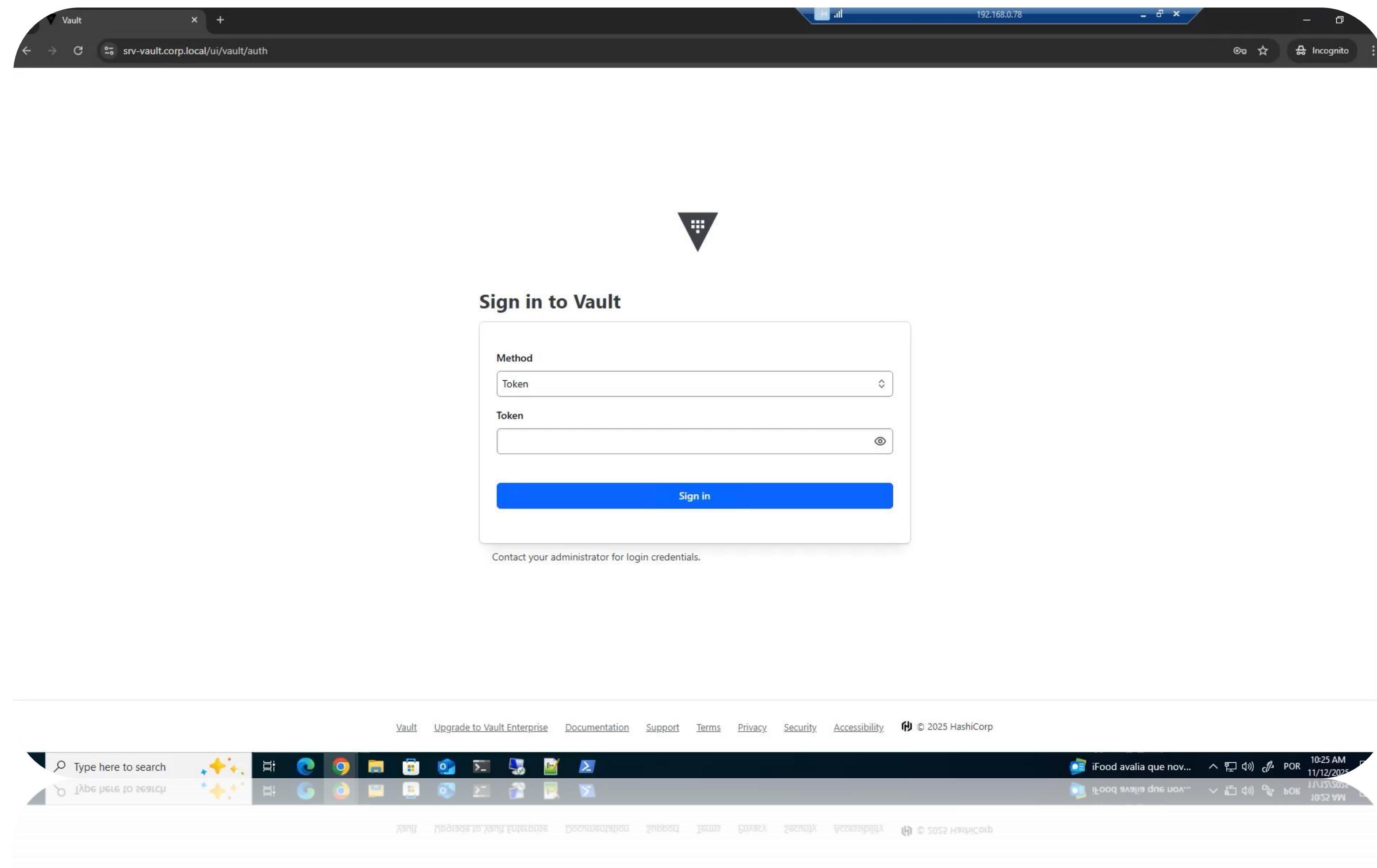
Demonstração: o cofre em ação

- Cenário: acesso válido às credenciais usando Passkey



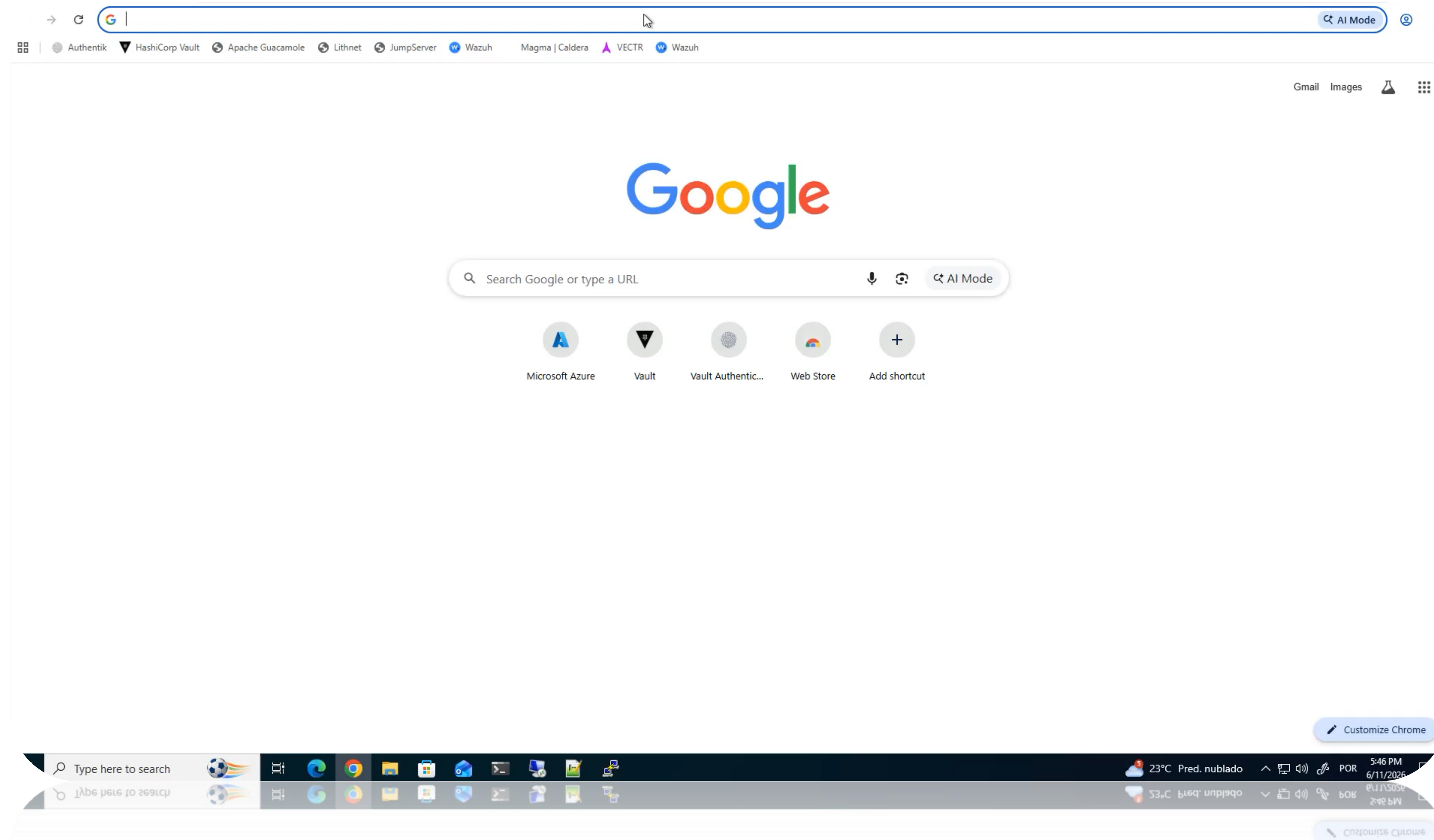
Demonstração: o cofre em ação

- Cenário: primeiro acesso de um usuário



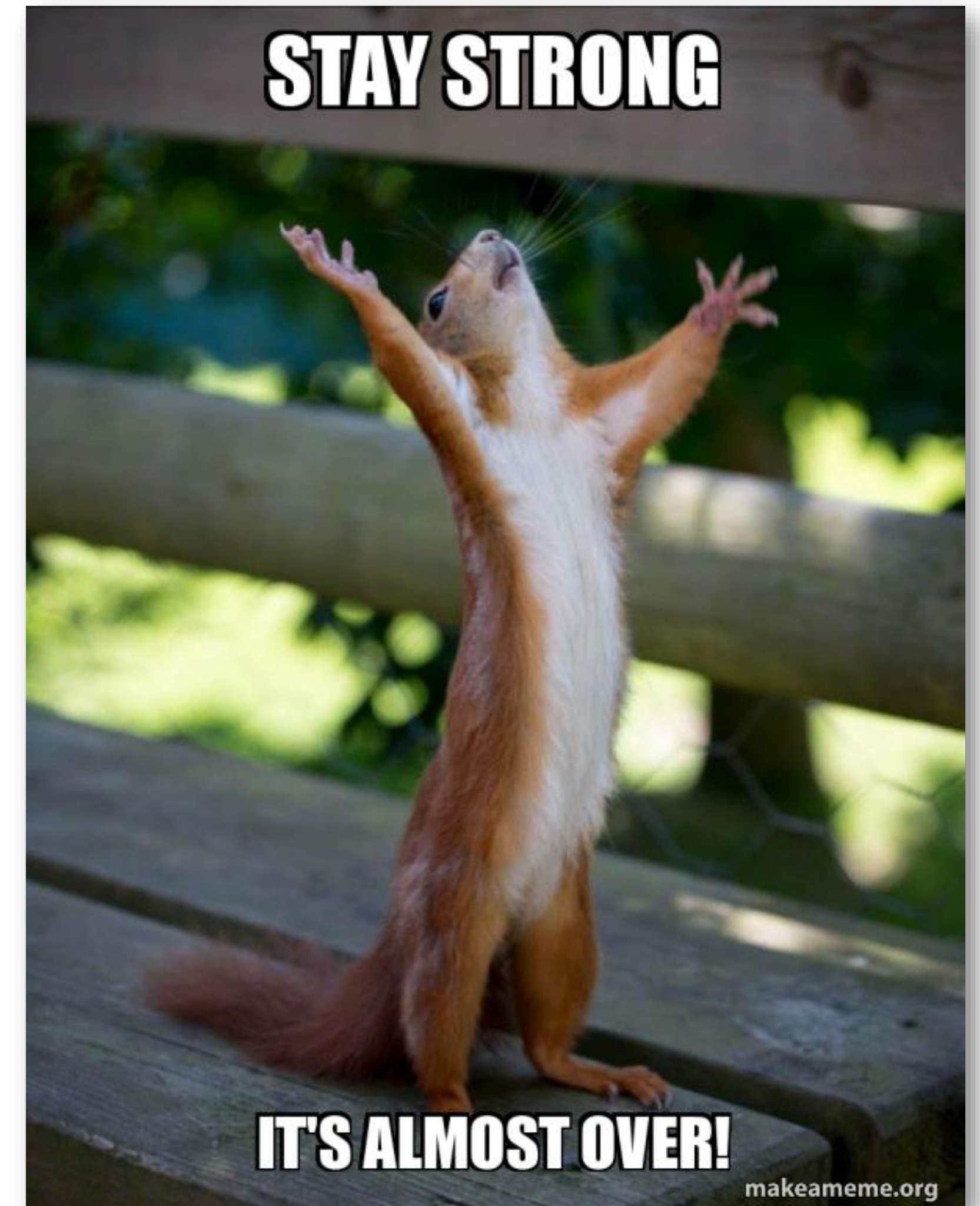
Demonstração: o cofre em ação

- Cenário: usando **outro IdP** (Entra ID)



Conclusão e próximos passos

- Gestão de senhas de contas privilegiadas ✓
 - Senhas temporárias (1h) e complexas
- Problema ✗
 - Se máquina do cliente está comprometida, senhas são vazadas (*clipboard*)
- Como resolver?
 - PAW (raro)
 - Integração do Vault com ferramentas de acesso remoto
 - Ex: Apache Guacamole ou JumpServer



O jogo ainda não terminou...

GUACAMOLE-2196: Openbao/Hashicorp Vault extension #1214

Code ▾

 **Closed** [adb014](#) wants to merge 16 commits into [apache:main](#) from [adb014:openbao](#) 

 Conversation 21  Commits 16  Checks 0  Files changed 31

+3.257 -3 

GUACAMOLE-2196: Add documentation for OpanBao, HashiCorp Vault #292

Code ▾

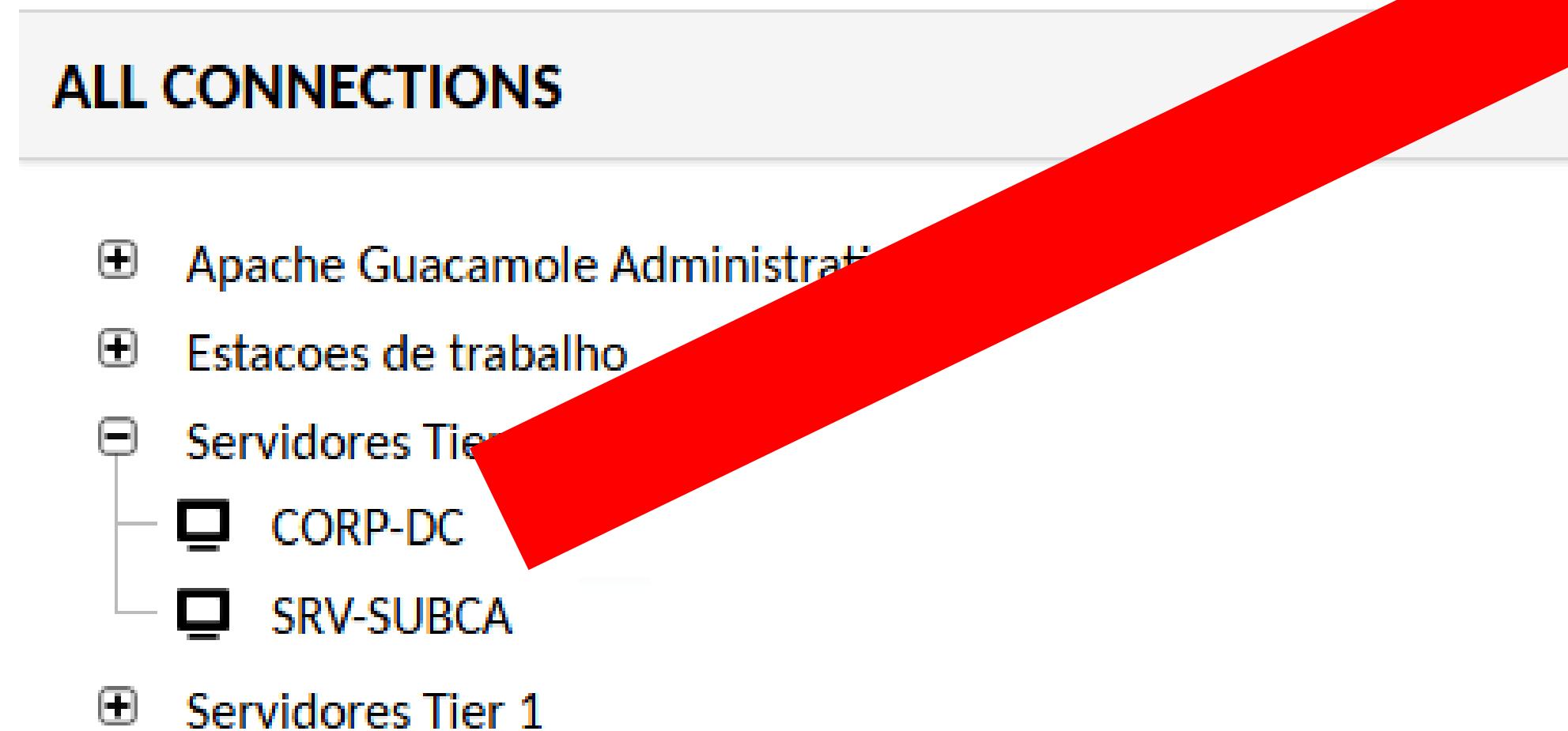
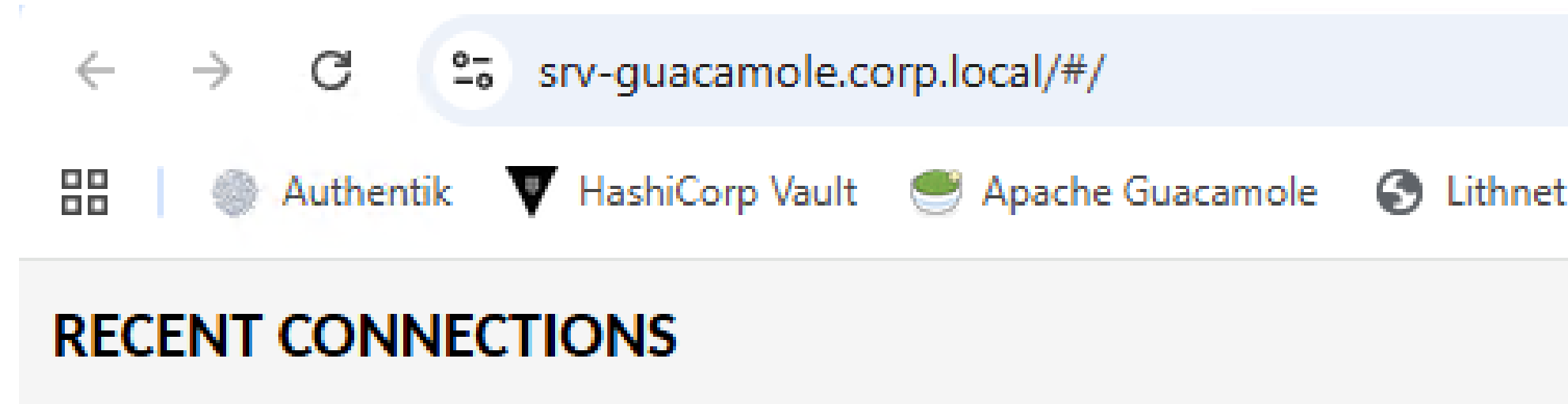
 **Closed** [adb014](#) wants to merge 2 commits into [apache:main](#) from [adb014:openbao](#) 

 Conversation 1  Commits 2  Checks 0  Files changed 6

+1.578 -13 

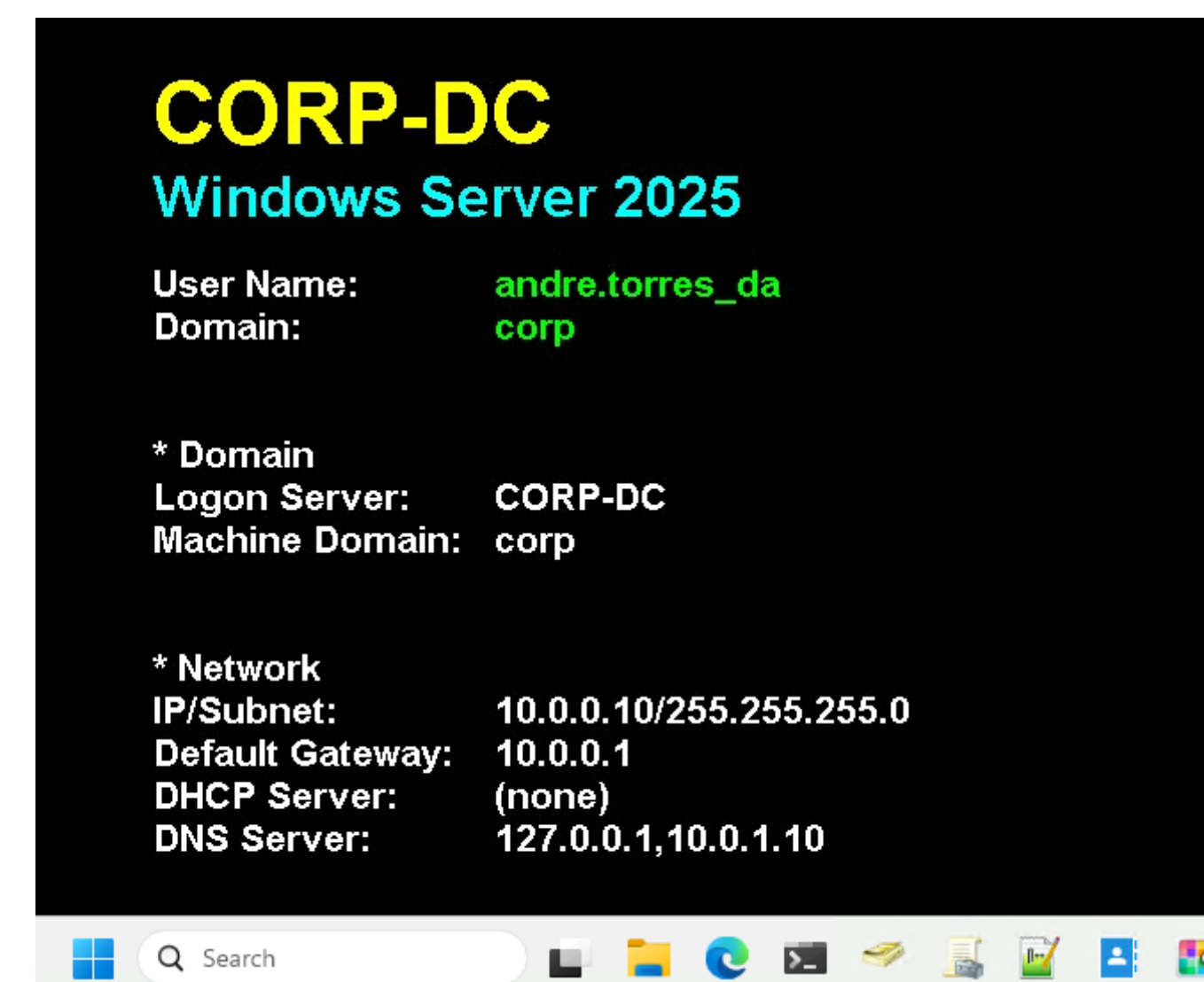
O jogo ainda não terminou...

Usuário: **andre.torres**



Usuário: **`${GUAC_USERNAME}_da`**

Senha:  **Vault**



Obrigado 😊



André Torres

<https://www.linkedin.com/in/andretorresbr/>