



# Técnicas para dar mais segurança à sua plataforma TOTVS Fluig: 5 dicas práticas

» Abner de Assis Athayde  
Rafael Maciel Vanat

A large, glowing circular graphic with a multi-colored aura (purple, blue, yellow) surrounding the text.

UNIVERSO  
TOTVS  
2024



## A importância da segurança

Prejuízo financeiro; Impacto na credibilidade; Perda de valor de mercado;  
Perda de dados pessoais e corporativos.



**38%**

Aumento de ciberataques no Brasil no primeiro trimestre de 2024.



**74%**

Origens Internacionais. Brasil está entre em 2o lugar no *ranking*.

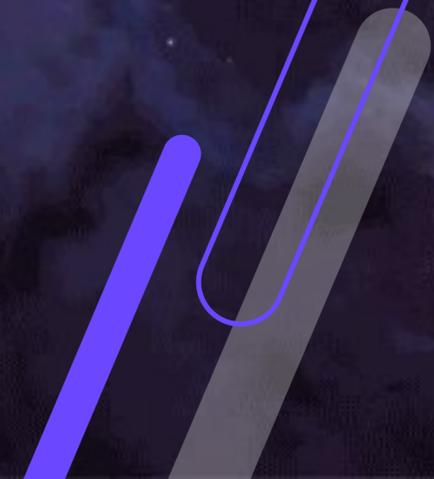


**R\$5,8M**

aproximadamente de prejuízo/ano.



# TOTVS Fluig: o que é?





**A solução que potencializa  
a **produtividade** da sua empresa.**



## Nossas **soluções** de produtividade

Gestão de Processos;  
Gestão de Documentos;  
Gestão de Portais;  
Rede Social Colaborativa;  
Geração de Indicadores;  
Gestão de Acessos.





# 20 milhões

*de usuários espalhados pelo mundo*





# 01 Proxy reverso

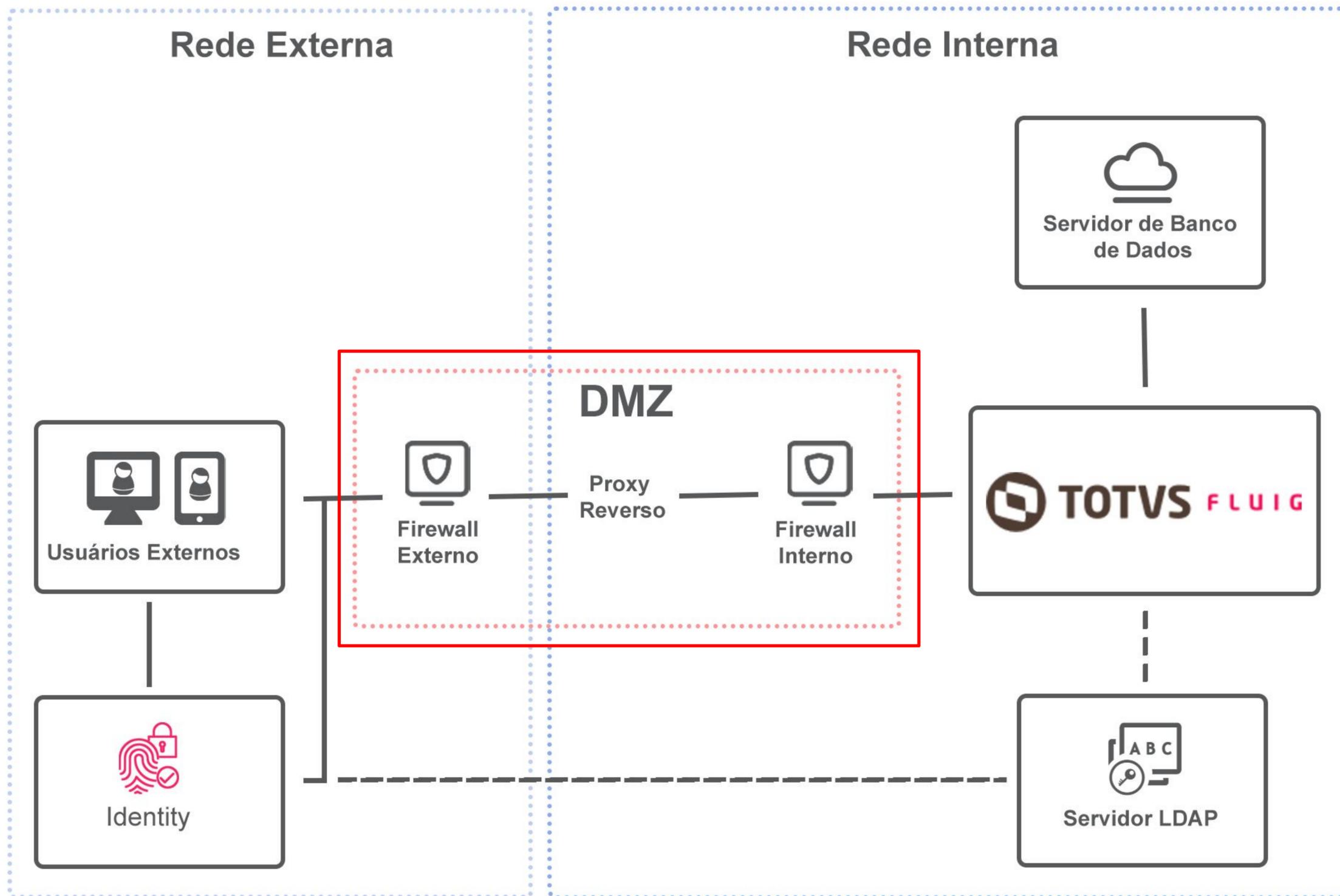
Segurança, Escalabilidade e  
Manutenção Simplificada



# Proxy reverso - Zona Desmilitarizada (DMZ)



Arquitetura com menor exposição



# Proxy reverso - Zona Desmilitarizada (DMZ)

Segurança, confiabilidade, facilidade de manutenção



<httpd.apache.org>

## Benefícios:

- O servidor de aplicação **não fica exposto** diretamente à rede;
- Viabiliza a implementação de **novos recursos e níveis de segurança** a qualquer momento, sem a necessidade de manutenção na aplicação em si, como por exemplo aplicação de SSL;
- Facilita a **escalabilidade** com o balanceamento de carga;



**NGINX**  
PROXY MANAGER

<nginx.org>

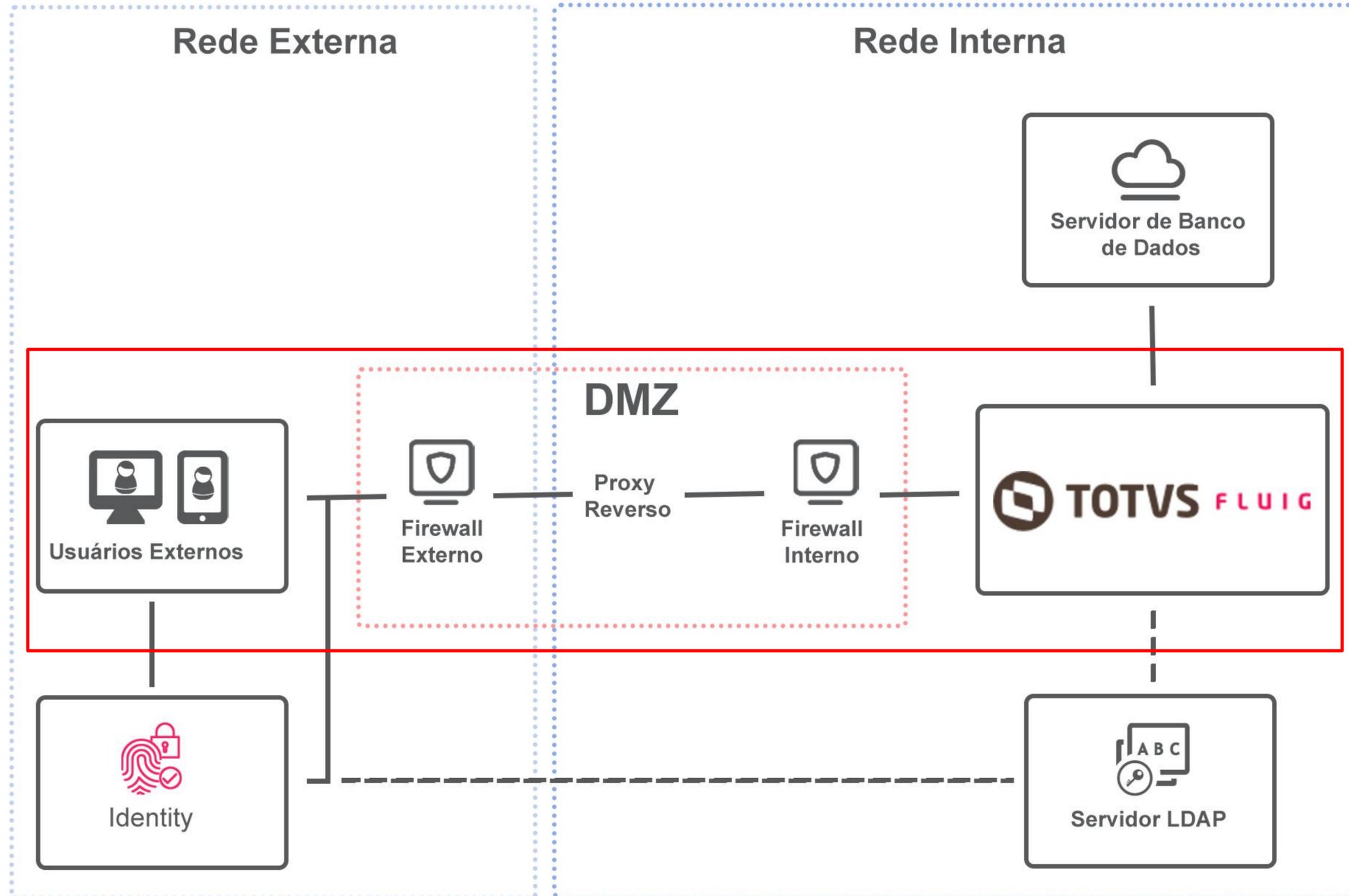
# 02

# HTTPS

Segurança e Privacidade Online



## Segurança de Ponta a Ponta na Web



# Configuração **HTTPS** da plataforma

Sobre os certificados



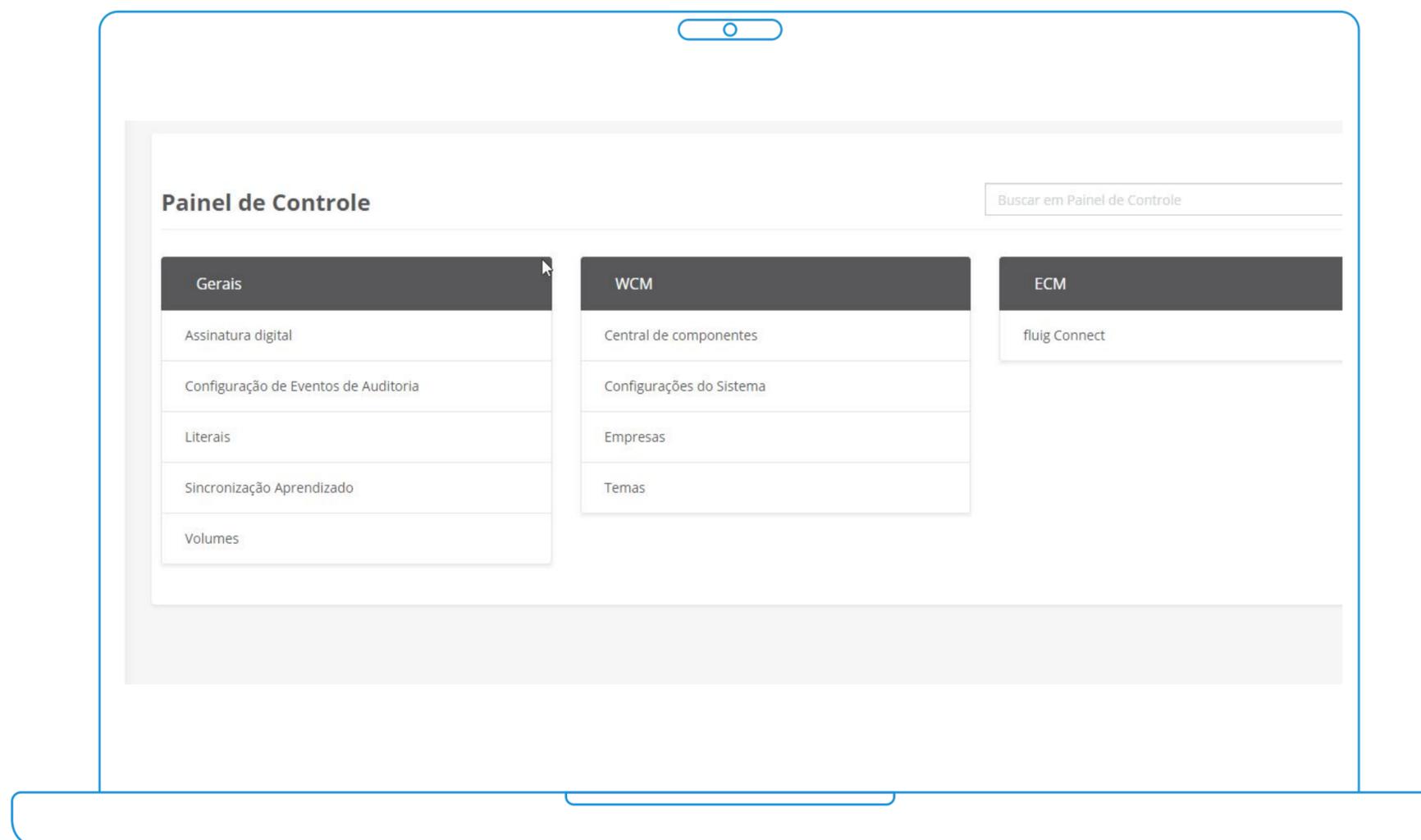
## Cuidados:

**Certificados:** Deve ser emitido para **domínios específicos** ou hosts dentro desses domínios.

(Exemplo: \*.suaempresa.com.br).

**Aquisição:** Certificados devem ser adquiridos de **autoridades certificadoras confiáveis**.

**Validade:** Certificados têm data de expiração, é **importante renová-los** antes do vencimento.



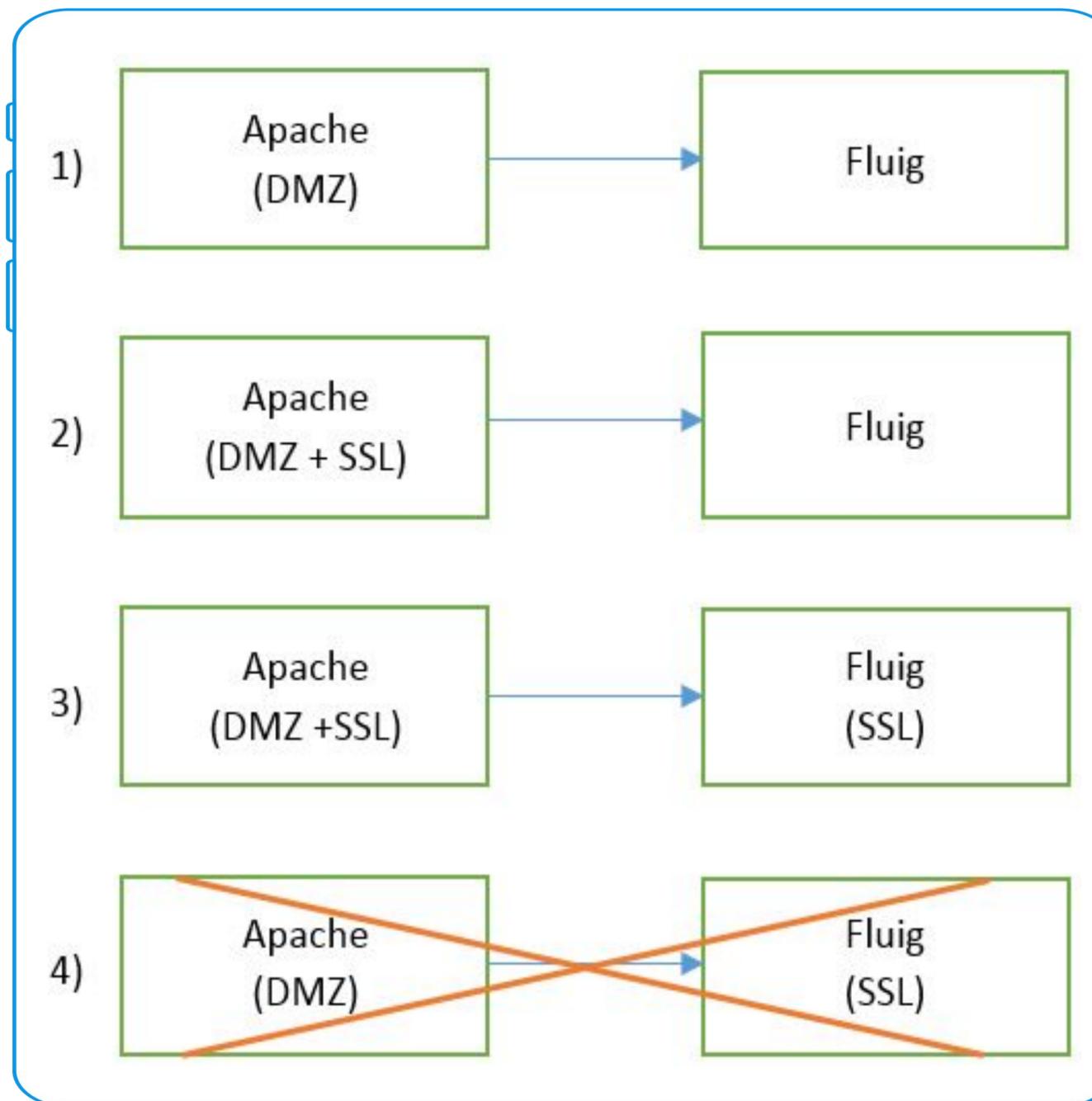
# Configuração de Proxy Reverso / DMZ



## Topologias

Alguns exemplos de topologias de DMZ e SSL com a plataforma TOTVS Fluig.

Mais recomendada considerando segurança e desempenho.



03

# Gestão de acessos e senhas

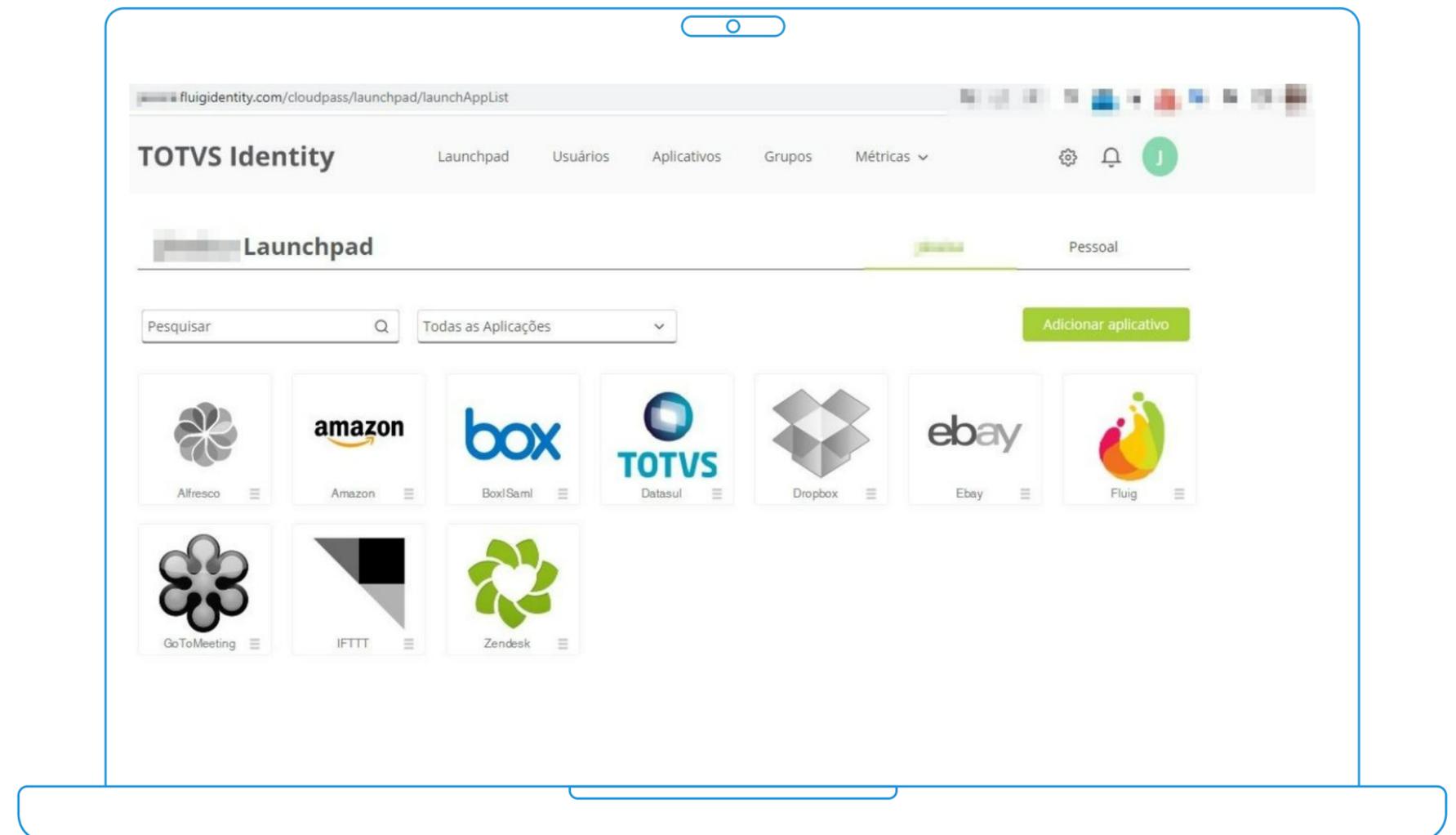
Garantia de proteção, segurança e controle de acessos



Gerenciamento centralizado de login e senha para múltiplos sistemas

## Principais recursos:

- Gestão Centralizada
- Proteção de Informações
- Integração ao AD (SmartSync)
- Integração Azure
- Single Sign-On
- Política de Senhas
- Self-Service de Reset de Senha
- Segurança com captcha
- Autenticação de duplo fator (MFA)
- Conformidade Legal (LGPD e Lei Sarbannes-Oxley)
- Auditoria de Acessos



# Configuração LDAP

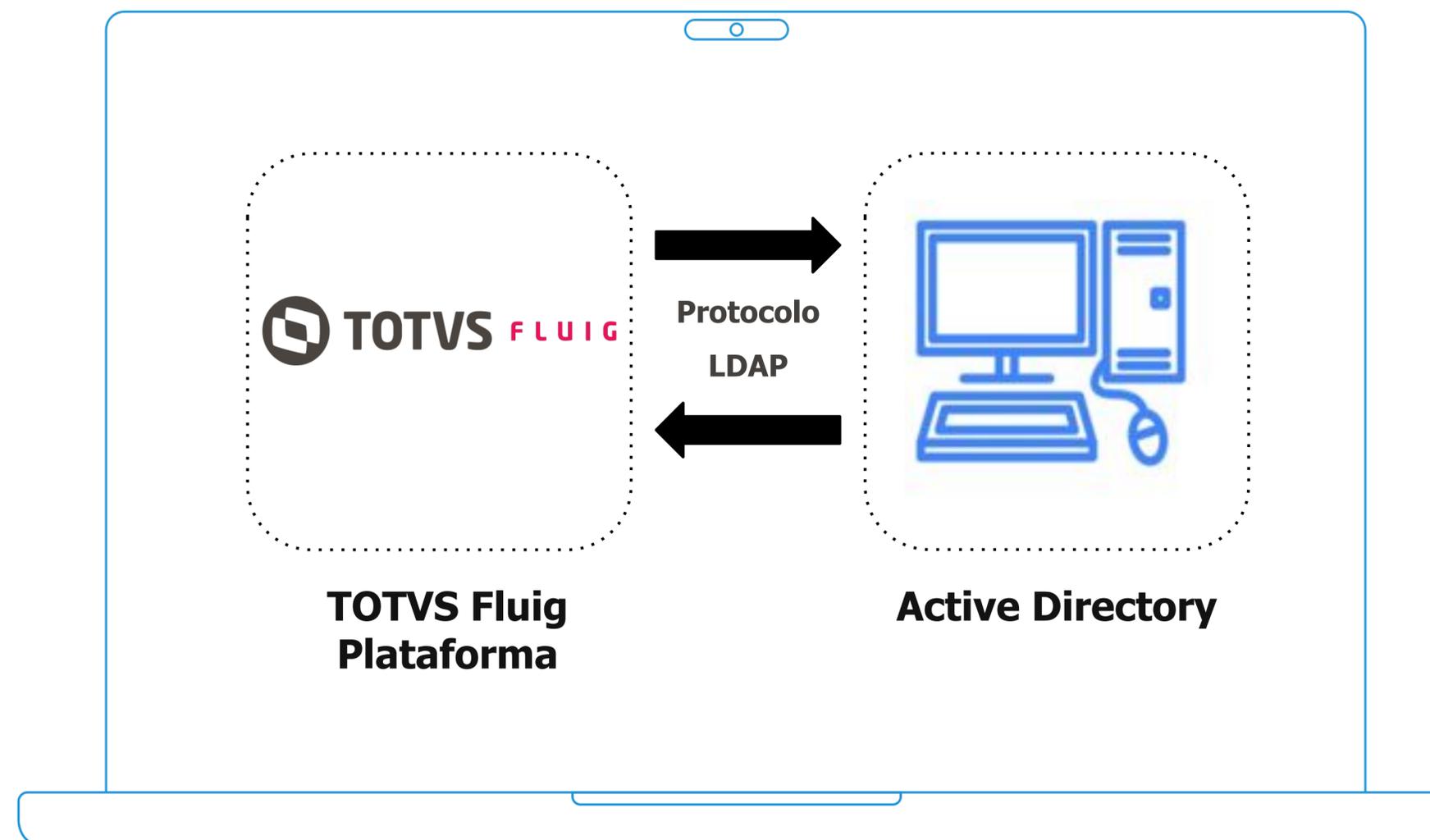
LDAP (Lightweight Directory Access Protocol)



**LDAP:** Protocolo para comunicação com o Active Directory.

**Centralização de Acessos:** Valide as credenciais dos usuários do TOTVS Fluig diretamente no AD.

**Políticas de Segurança:** Respeite políticas já utilizadas do seu AD.



## O que são Eventos Globais?

Os eventos globais do TOTVS Fluig são executados pela plataforma **antes ou após alguma ação ocorrer** e podem ser personalizados através da linguagem Javascript.

## Regras que podem ser implementadas:

- **Complexidade e Expiração de Senha:** Configure regras que exigem senhas fortes e com prazo de expiração.
  - **beforeCreateUser:** Evento disparado antes da criação de um novo usuário.
  - **beforeUpdateUser:** Evento disparado antes da atualização de um usuário.
- **Prevenção de Ataques de Força Bruta:** Configure bloqueios após várias falha tentativas de login.
  - **onLoginError:** Evento disparado quando ocorrer um erro de login de um usuário. Podendo também exibir alertas



### Exemplo de implementação:

```
function beforeCreateUser(user) {  
  
    // Verifica se a senha informada atende os requisitos mínimos  
    var passwordPattern = "((?=.*\\d)(?=.*[a-z])(?=.*[A-Z])(?=.*[@#$%]).{8,16})";  
    if (!user.getPassword().matches(passwordPattern)) {  
        throw "A senha do usuário não atendeu os requisitos mínimos!";  
    }  
  
    // Adiciona um dado adicional ao usuário informando a sua data de criação  
    var dateFormat = new java.text.SimpleDateFormat("dd/MM/yyyy HH:mm:ss");  
    user.putData("CreationDate", dateFormat.format(new Date()));  
  
}
```

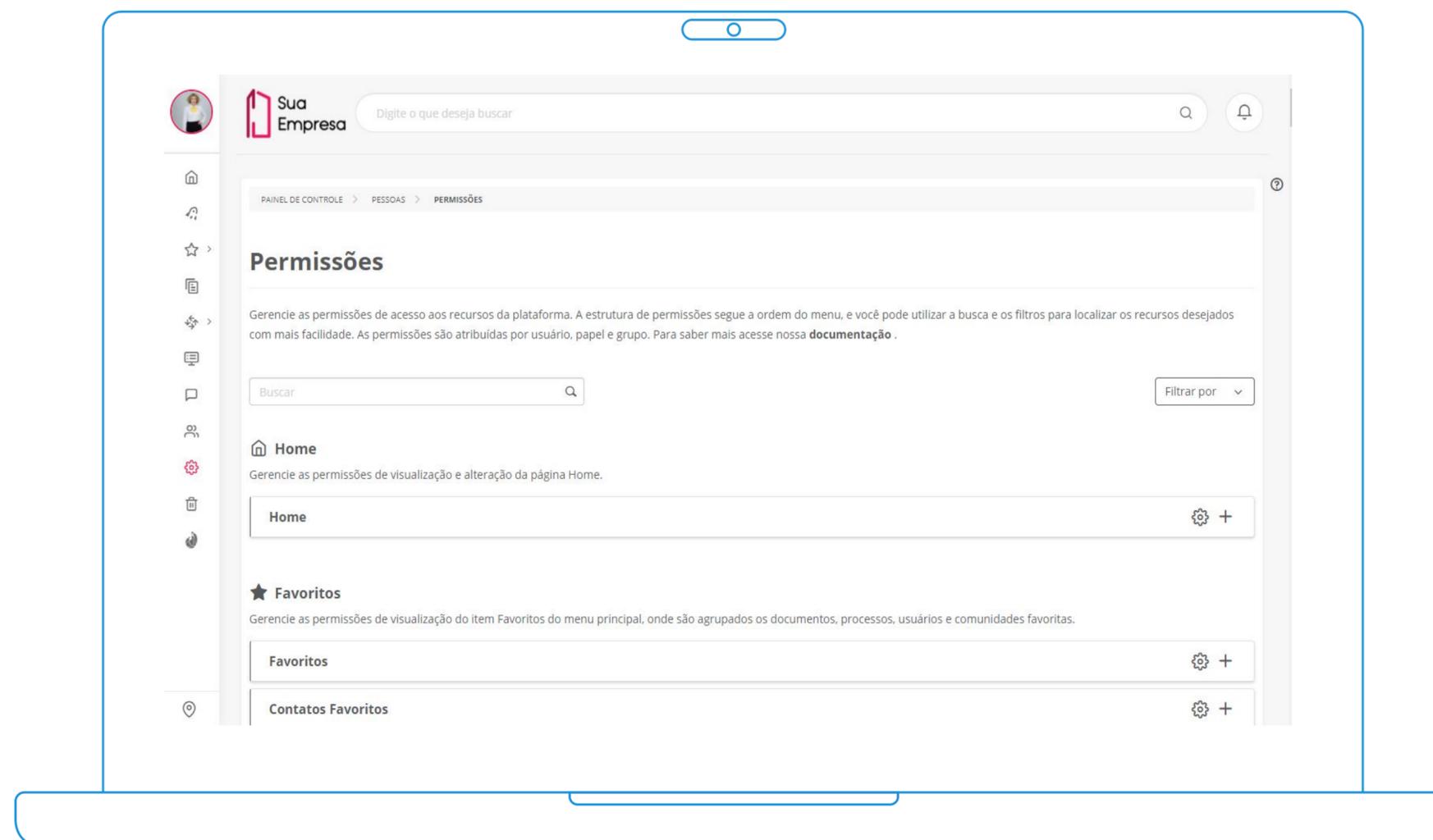
# Gerenciar acesso aos **documentos**

Foco na gestão digital

- Crie uma organização lógica para os documentos (**Taxonomia**);
- Defina as permissões **específicas** para as pastas e documentos;
- **Facilite** com o uso de **herança** das permissões;
- Controle a **aprovação** de documentos;
- **Oriente** os usuários na correta definição de segurança;
- Atenção com a permissão **TODOS**;
- A busca do TOTVS Fluig **respeita** o acesso do usuário;



- Papel user e **admin**;
- **Atribua permissões** a determinados usuários, papéis e grupos;
- Gerencie os recursos:
  - Sociais e de comunidades;
  - Documentos;
  - Processos;
  - APIs, datasets internos e webservices;
  - Páginas;
  - Barra de pesquisa e ícone de notificações;
- **Emita relatório** de permissões;
- **Restaure o padrão** de permissões;



## Situação:

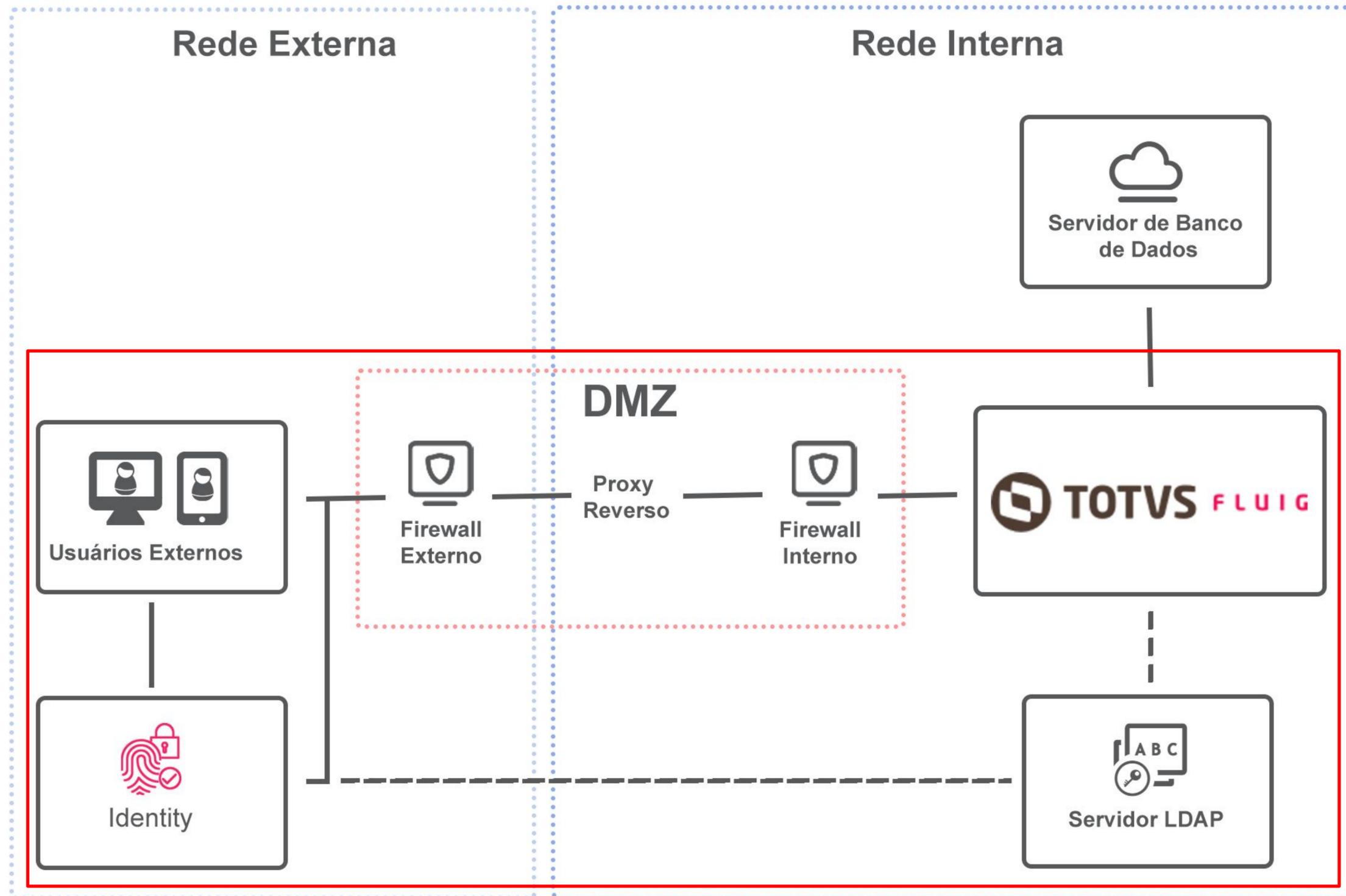
- **Exposição de credenciais** em código-fonte, principalmente em código *clientside* (no lado do navegador).
  - Dê preferência ao **cadastro de serviços** para gerenciar a autenticação.
- Expor APIs completas de forma pública **sem limite** de recursos.
  - Crie uma API **intermediária**, que possua apenas alguns recursos.
- Uso não **planejado de papel administrador** para integrações.
  - Usuário para autenticação na API que possua **acesso apenas aos recursos necessários**.





# Gestão de acessos e senhas

Organização e segurança do seu ambiente



04

# Backup e criptografia

Garantia e proteção de senha do banco de dados





# Backup e Encriptação de Senha



Importante recurso remediativo

## Benefícios:

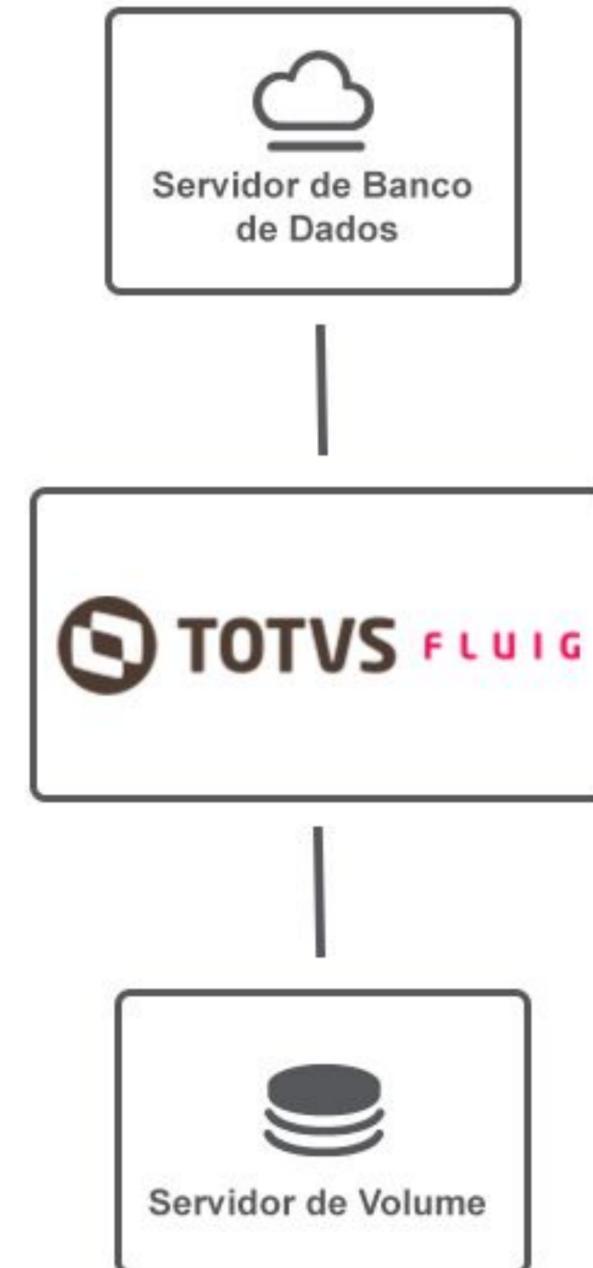
- A melhor **defesa** contra a perda de dados.
- **Reduza o risco** de violações de dados e ransomware.
- Garanta a **continuidade** dos negócios em caso de incidentes.

## Encriptação de Senha do Banco:

Aumente a segurança das suas informações. **Evite o acesso não autorizado à base de dados.**

## Etapas da encriptação:

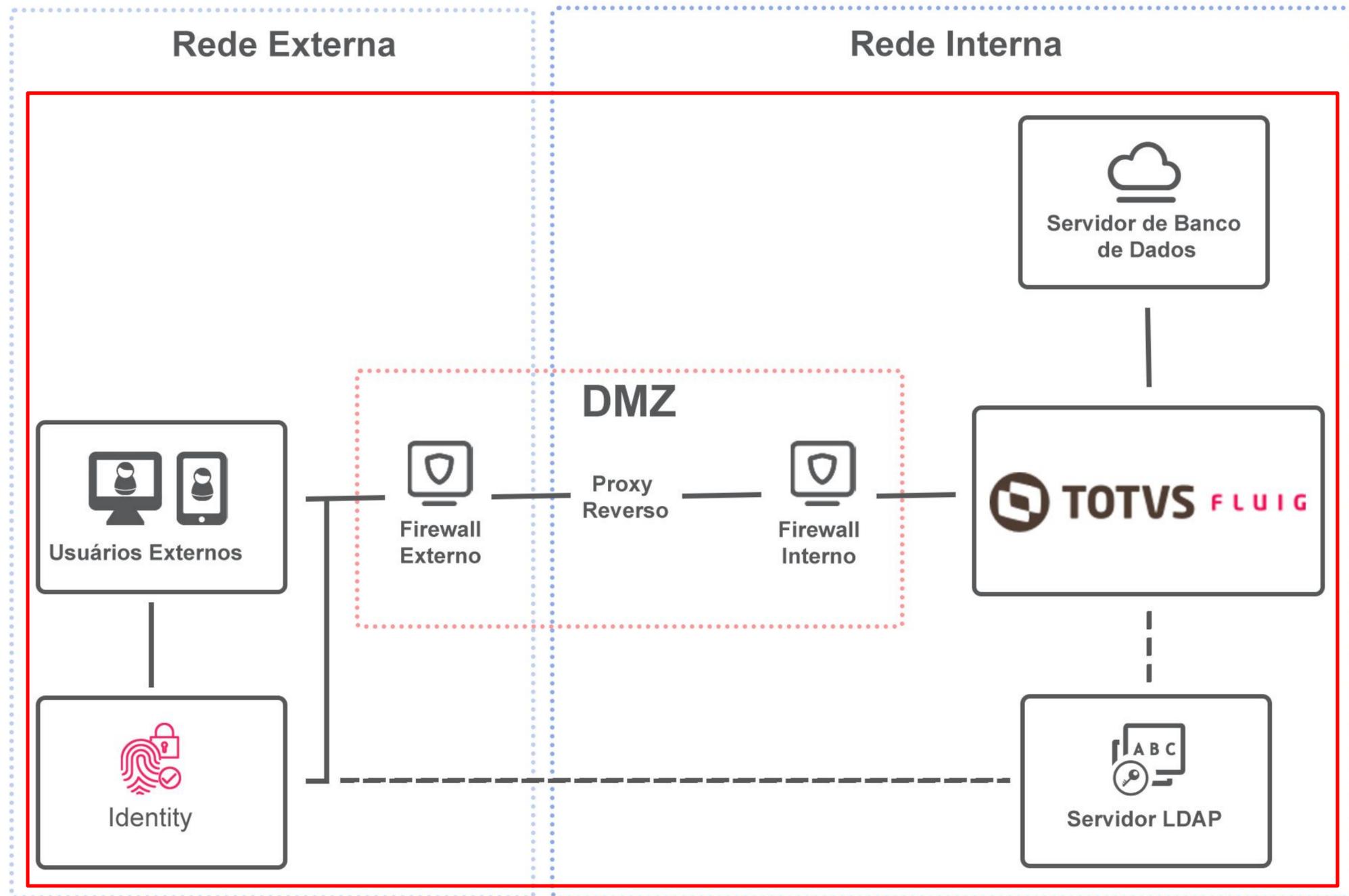
- **Encriptação da senha da base de dados (DataSource)**
  - Comando simples executando um jar da plataforma.
- **Criar a política de autenticação da aplicação com a senha encriptada**
  - Alteração do arquivo de configuração domain.xml





# Backup e criptografia

Prevenir e Remediar



05

# Atualização da Plataforma

Manutenção e segurança em dia





# Atualização da Plataforma



Mantenha-se em segurança

Ações de segurança: levamos em consideração as **recomendações da OWASP**.

Testes de vulnerabilidades: empresas terceiras realizam **Pentests regulares** e de forma independente.

Agilize o seu suporte: manter-se atualizado **reduz o tempo de atendimento**.



**Selo Update**, correções referente a tickets abertos por clientes e pequenas melhorias.

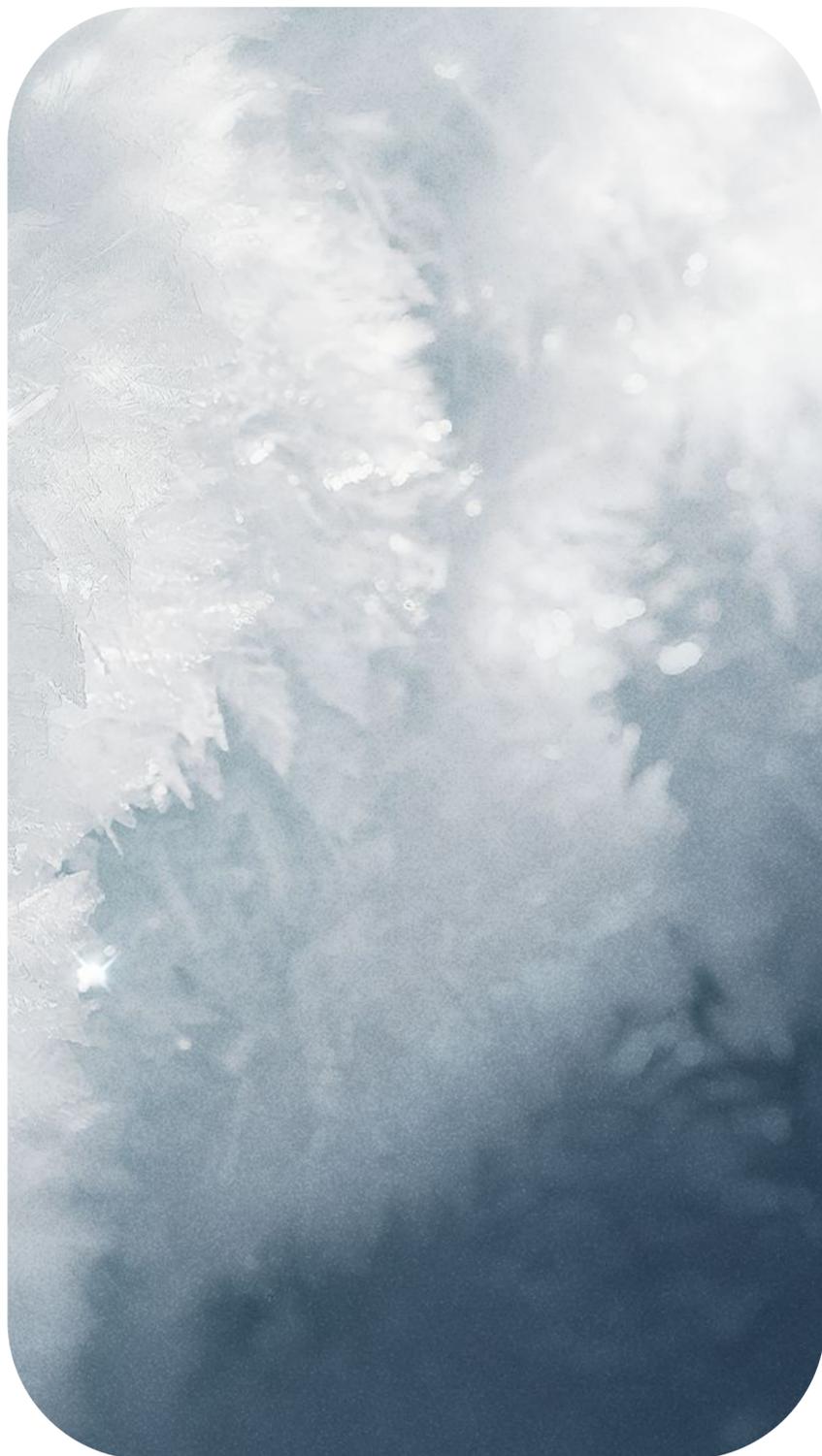


**Selo Essential**, correções e algumas melhorias de destaque: benefícios para o dia a dia da sua empresa.



Atenção ao **selo Mandatory!**

Correções críticas e de segurança, altamente recomendada a atualização para as correções serem refletidas em seu ambiente.



# Crystal Mist

## Release 1.8.2

Participe do evento no qual os nossos especialistas de produto apresentarão as inovações da nova *release* e estarão disponíveis para esclarecer todas as dúvidas.

Fortaleça a sua conexão com o nosso time e fique por dentro de todas as novidades. **Inscreva-se agora!**

**Evento gratuito e online.**

**Data:** 10/07/2024 às 15h.

**Inscrição:** <https://bit.ly/NovaRelease>





+ **Bônus: Eventos de Auditoria**

Análise Detalhada de Atividades





# Evento de Auditoria

## Análise Detalhada de Atividades



- **Plataforma:**
  - Datasets
  - Usuários, Grupos e Papéis
- **Processos:**
  - Versionamento
  - Conversões
  - Substitutos
  - Anexos
- **Documentos:**
  - Criação, Revisão, Exclusões, Restauração e Downloads
  - Limpeza Lixeira
- **Pesquisa e Exporte Resultados**

Panel de controle / Eventos de Auditoria

### Eventos de Auditoria

**Atenção:** Os eventos poderão levar até 5 minutos após sua ocorrência para estarem disponíveis para consulta.

Busca de Eventos

Digite o nome do usuário

Informe o recurso Informe a chave Período de 08/05/2018 até 08/05/2018 **Buscar**

Resultado de Busca

Usuário	Evento	Recurso	Data/Hora	Chave	Salva Mais
Administrador fluig	Edição	Papel	08/05/2018 às 15:19:08	user	Q
Administrador fluig	Criação	Usuário	08/05/2018 às 15:19:08	jose	Q
Administrador fluig	Edição	Papel	08/05/2018 às 15:21:06	user	Q
Administrador fluig	Criação	Usuário	08/05/2018 às 15:21:06	maria	Q
Administrador fluig	Criação	Criação de pasta	08/05/2018 às 16:50:48	102	Q
Administrador fluig	Criação	Criação de documento	08/05/2018 às 16:50:54	103	Q
Administrador fluig	Criação	Criação de pasta	08/05/2018 às 16:51:06	104	Q
Administrador fluig	Edição	Criação de versão	08/05/2018 às 16:51:43	103	Q

**Exportar Dados** << >>



# Evento de Auditoria



Detalhe de Atividade ✕

Nome do usuário	Login do usuário
adm adm	adm
Endereço IP	Recurso
10.80.73.66	Grupo
Evento	Chave
Criação	Recursos Humanos
Data/Hora	
06/03/2018 às 14:03:33	
Descrição da Atividade	
Criação do grupo Recursos Humanos com descrição Grupo destinado à assuntos de RH e tipo user	

Fechar

Detalhe de Atividade ✕

Nome do usuário	Login do usuário
adm adm	adm
Endereço IP	Recurso
10.80.73.66	Papel
Evento	Chave
Criação	papel.rh.folha
Data/Hora	
06/03/2018 às 14:10:48	
Descrição da Atividade	
Criação do papel papel.rh.folha com a descrição Folha de Pagamento	

Fechar

# Recapitulando



# /// Recapitulando

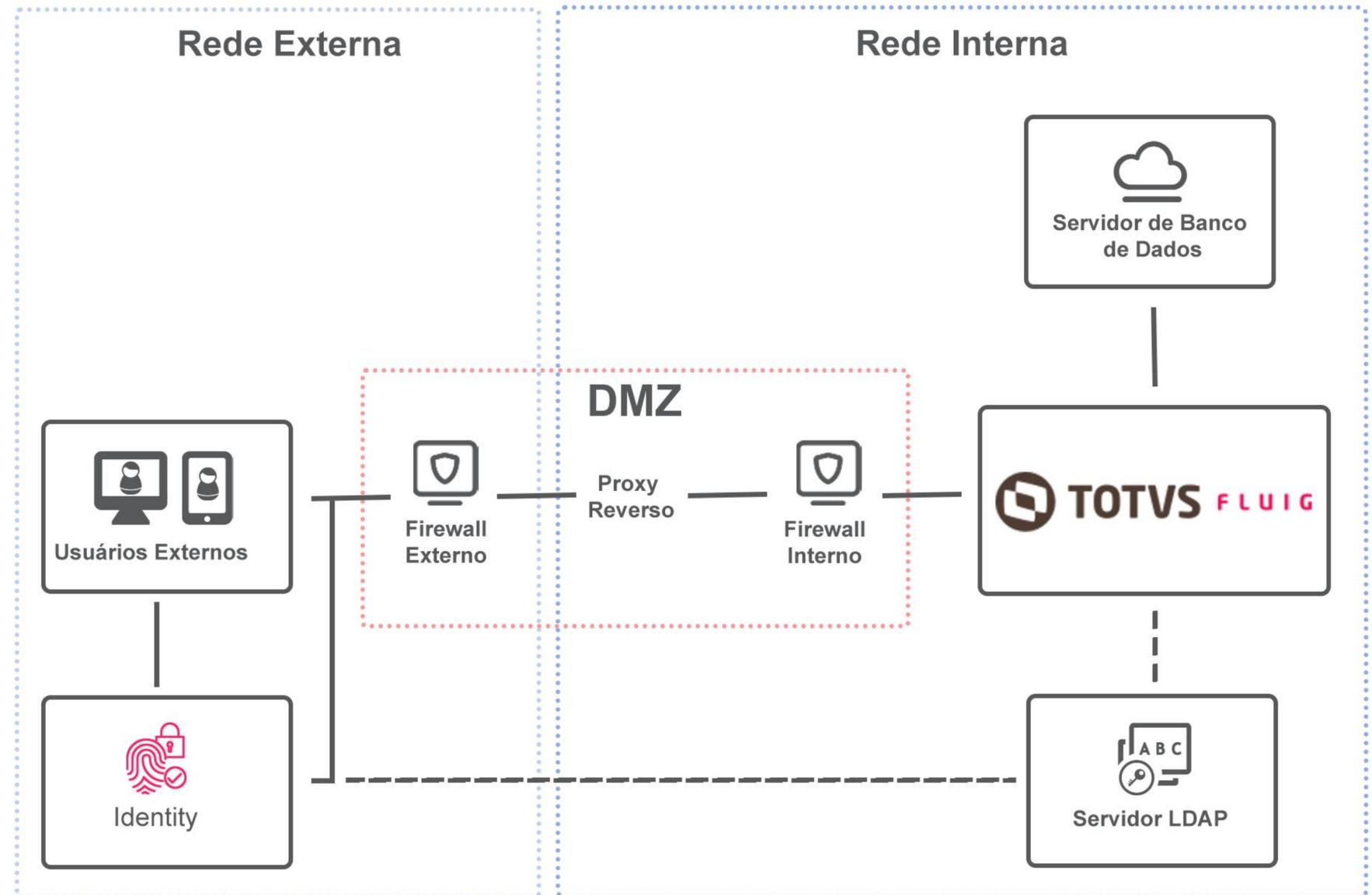
Cuidar para não precisar remediar

- Proxy Reverso
- Protocolo HTTPS
- Gestão de acessos e senhas
- Backups
- Atualização
- ★ Eventos de Auditoria

Material de Apoio:



<https://bit.ly/FluigSeguro>



# Precisa de apoio?

A gente te ajuda!



# O Works oferece tudo para você não se preocupar.

Por meio de uma assinatura, você tem acesso a horas de especialistas para auxiliar na criação e na evolução do seu ambiente.

Como funciona?

**1**

Você escolhe um plano com a quantidade de atendimentos essenciais para as suas necessidades.

**2**

Um parceiro será designado para atendê-lo.

**3**

O mesmo parceiro atenderá durante todo o contrato.<sup>1</sup>



Os parceiros oficiais Works tem selo de qualidade TOTVS Fluig.

Escolha como as suas horas serão utilizadas:

## desenvolvimento, treinamento, apoio e sustentação.

Temos o **pacote ideal**, pronto para atender às suas necessidades.



Flows essenciais

Limite de horas anuais

Atendimento executado por

Essential

Standard

Advanced

Professional

Enterprise



48h

96h

192h

288h

576h

Parceiro ou TOTVS

O nosso pacote básico.

Pacote para um apoio mais abrangente.

Pacotes para quem tem espaço e necessidade de investir em desenvolvimento.

Todos os pacotes dão direito a **todos** os Flows Essenciais disponíveis.

<sup>1</sup> Trocas podem ocorrer caso: o parceiro deixe de atender via Works; não renove sua parceria com a TOTVS.



# PRIME Fluig

Diferenciais - PARCERIA



## Monitoramento de Desempenho

Identificamos ofensores no Desempenho e indicamos melhorias nos desenvolvimentos, Infraestrutura ou configurações



## SLA Agressivo

Telefone Vermelho entre Cliente e Especialista. Realizamos a Gestão do Suporte do cliente.



## FIT Cultural

Conhecimento das regras de negócio do cliente



## ROI

Redução de Carga da TI e Projeto



## Consultoria para Desenvolvimentos

Apoio Consultivo para novos desenvolvimentos. Segurança nas atualizações (Widgets, Processos, Formulários e Integrações).

## SUPORTE PADRÃO X PRIME

	SUPORTE À DÚVIDAS	SUPORTE AOS INCIDENTES NOS DESENVOLVIMENTOS SOBRE A PLATAFORMA	MONITORAMENTO DO DESENVOLVIMENTO	CONTATO DIRETO COM ANALISTAS	SLA REGRESSIVO
SUPORTE PADRÃO	✓	✗	✗	✗	✗
SUPORTE PRIME	✓	✓	✓	✓	✓

# /// Acompanhe o Fluig no Universo TOTVS



Confira mais horários de apresentações e o nosso estande

DATA	TRACK	LOCAL
 <b>19/06</b> 12h00 - 12h45	10 dicas para turbinar seu TOTVS Fluig, melhorando desempenho e estabilidade	 CODE NO CODE 4
 <b>19/06</b> 14h00 - 14h45	Simplifique a gestão de senhas e MFA com o TOTVS Identity	 CODE NO CODE 1
 <b>19/06</b> 14h00 - 15h45	Wargame: tenha uma experiência de como responder a um Cyberattack*	 CODE NO CODE PRO 2



## ESTAMOS NOS ESTANDES 50 e 51!

Venha conversar conosco 😊

\*Conteúdo pago separadamente

# OBRIGADO



**Abner A. Athayde**

Especialista - Suporte Prime Fluig  
abner.athayde@fluig.com



**Rafael M. Vanat**

Coordenador – Suporte Fluig  
rafael.vanat@fluig.com



[totvs.com](http://totvs.com)



[@totvs](https://www.instagram.com/totvs)



[@totvs](https://twitter.com/totvs)



[@somostotvers](https://www.instagram.com/somostotvers)



[/totvs](https://www.youtube.com/totvs)



[/totvs](https://discord.com/channels/123456789/123456789)



[totvs.store](http://totvs.store)



[company/totvs](https://www.linkedin.com/company/totvs)



**Valorizamos gente boa que é boa gente**



**Somos movidos por resultados**



**Investimos na tecnologia que viabiliza**



**Construímos relações de longo prazo com nossos clientes**



**Quando colaboramos somos mais fortes**

**#SOMOSTOTVERS**

