# CASO DE SUCESSO

Como o **Segura®** transformou o acesso privilegiado na FIEMA

## FEDERAÇÃO DAS INDÚSTRIAS DO ESTADO DO MARANHÃO

segura®

# SUMÁRIO


| | |
|---|---|
| SUMÁRIO | 1 |
| RESUMO EXECUTIVO | 2 |
| DESAFIOS | 4 |
| SOLUÇÕES | 6 |
| RESULTADOS | 8 |
| OPINIÃO DOS USUÁRIOS | 10 |

# RESUMO EXECUTIVO

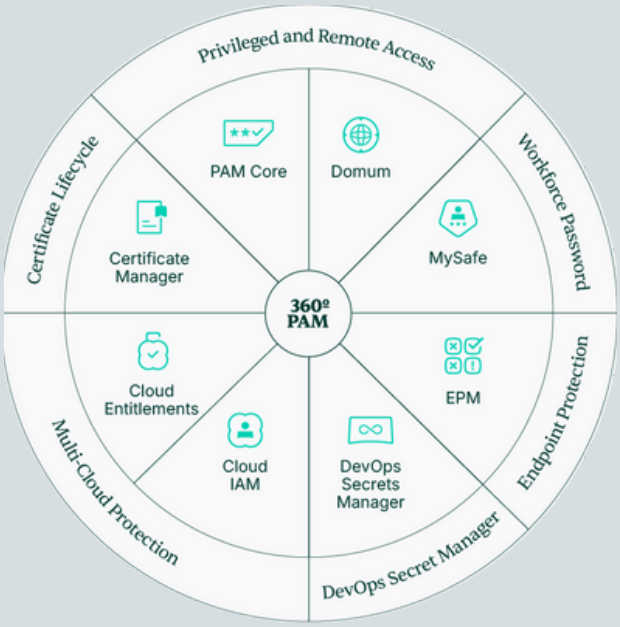
Este documento apresenta o caso de sucesso na adoção do **Segura®** como solução de Gerenciamento de Acesso Privilegiado - PAM na **Federação das Indústrias do Estado do Maranhão (FIEMA)**.

Com a modernização tecnológica e o aumento da oferta de serviço digitais, a gestão de acessos se tornou mais complexa e dinâmica.

Os acessos com **privilégios administrativos (acessos privilegiados)** são particularmente sensíveis, pois, além do potencial de erros operacionais, há o alto índice de ataques focados na obtenção dessas credenciais que, uma vez obtidas, podem comprometer dados e serviços de forma irreversível ou até mesmo comprometer todo o ambiente de TI.

Portanto, a **Federação das Indústrias do Estado do Maranhão (FIEMA)** adotou uma solução para gestão dos acessos privilegiados, de forma a auditar, implantar cadeia de autorização, proteger as senhas e prover sessões seguras, mitigando os erros operacionais e o risco de vazamento de credenciais privilegiadas.

# SOLUÇÃO APRESENTADA




Como resultado do processo licitatório, ocorrido no dia 13 de junho de 2024, a **FIEMA** contratou a solução **Segura®**, que sagrou-se vencedora do certame por intermédio de sua parceira **ITware Soluções em TI**.

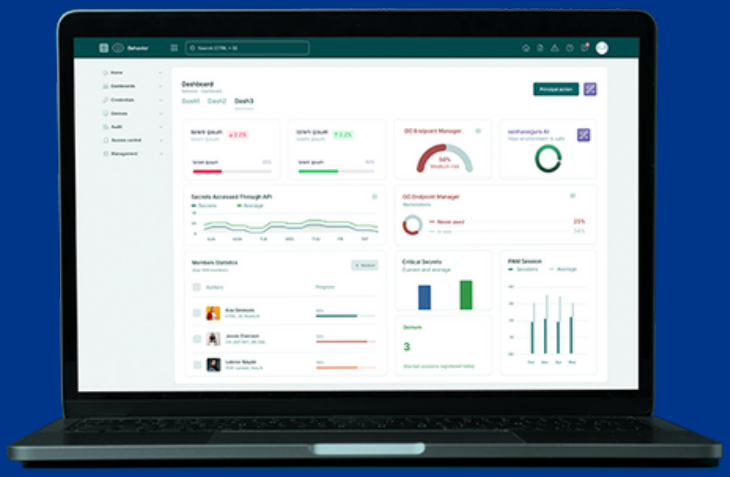
Para atender todos os requisitos exigidos no Edital, a **ITware Soluções em TI** forneceu uma proposta que engloba todos os módulos de gestão da **Segura®**. São eles:

- PAM Core
- Domum
- MySafe
- EPM
- A2A
- DevOps Secret Management
- Certificate Management

# PRINCIPAIS RESULTADOS

Na primeira fase do projeto de gestão de privilégios, a FIEMA adotou o **módulo de PAM Core**. Após uma implantação que durou **menos de 30 (trinta) dias**, foram alcançados os seguintes resultados:

- Segmentação de acesso por função;
- Habilitação de MFA para acessos privilegiados;
- Rotação automática de senhas privilegiadas locais e no Active Directory (senhas fortes);
- Proxy de sessão centralizado;
- Gravação de sessões RDP, SSH e HTTPS;
- Auditorias de sessões privilegiadas;
- Controle de execução de comandos em sessões privilegiadas.



# DESAFIOS

A FIEMA já utilizava o Active Directory para gestão de usuários, mas necessitava gerenciar os acessos privilegiados de forma a auditar, implantar cadeia de autorização, proteger as senhas e prover sessões seguras, mitigando os erros operacionais e o risco de vazamento de credenciais privilegiadas.

**Gestão de senhas**

As senhas privilegiadas eram criadas diretamente pela equipe de TI, sem o controle ou gestão da FIEMA. Muitas dessas senhas eram compartilhadas entre os usuários e qualquer alteração de equipe poderia causar uma troca de várias senhas. As trocas de senhas não eram documentadas e só eram realizadas em ocasiões especiais. Cada membro do time poderia escolher como manter a senha (decorada, anotada em blocos de notas, uso de cofre de senha pessoal etc.).

**Gestão de acessos**

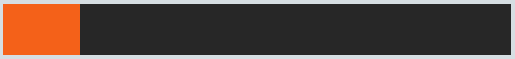
Os acessos privilegiados eram iniciados diretamente das estação dos administradores pelos protocolos padrões de gerenciamento. Qualquer usuário com conhecimento da senha privilegiada poderia acessar o servidor e/ou serviço. Uma vez que o acesso era realizado, não era possível controlar os comandos executados.

**Auditoria e controle**

A auditoria de acesso privilegiado se limitava aos logs de entrada (logins) e saídas (logoff). Uma vez que algumas senhas eram compartilhadas, não era possível individualizar esses acessos. As sessões privilegiadas não podiam ser auditadas, uma vez que não havia gravações ou registro dos comandos executados em sessões de administração.

## Metas para gestão de privilégios

Gestão de privilégios inicial




Meta de Gestão de privilégios

Com o uso do Active Directory, a FIEMA estima que alcançou a gestão de 15% (quinze por cento) dos acessos privilegiados.

Na **primeira fase**, com a implantação do **PAM CORE** a **FIEMA** pretende chegar a 75% (setenta e cinco por cento) da gestão de privilégios, implantando:

- Cofre de senhas seguro e criptografado;
- Regras para autorização de privilégios;
- Rotação de senhas após o saque;
- Entrega de sessão autenticada, sem que o usuário tenha contato com a senha;
- Individualização do acesso privilegiado;
- Registro de ações nas sessões privilegiadas;
- Permissão de auditorias de segurança;
- Rastreamento de uso de contas privilegiadas;
- Minimização do risco de vazamento e/ou uso de credenciais privilegiadas por usuários não autorizados;
- Minimização do risco de ataques de descoberta da senha por força bruta.

# EXPECTATIVA DA FIEMA

Finalizar a primeira fase da **gestão de acessos privilegiados**, solucionando os desafios de segurança para a equipe interna de TI da **FIEMA**.

É fundamental que a solução adotada não dificulte os acessos administrativos da equipe e nem provoque procedimentos complexos durante os acessos dos times de TI.

# SOLUÇÃO

Para a primeira fase do projeto de gestão de acessos privilegiados, a FIEMA implantou o módulo Segura® PAM Core, que irá gerenciar todos os dispositivos, usuários, senhas e sessões privilegiadas.

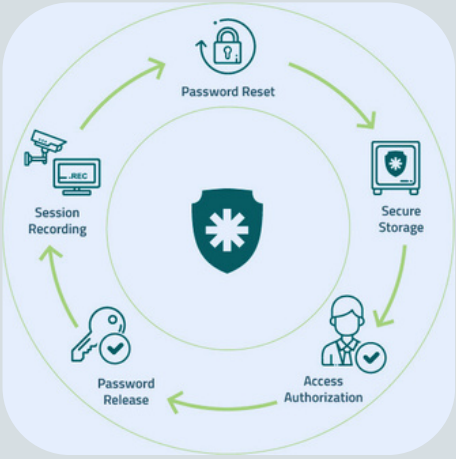
## GESTÃO DE ACESSOS E MFA

Um dos desafios da autenticação na interface PAM foi manter a simplicidade, incrementando os controles de segurança. Para isso, foram adotadas duas estratégias: integração com o Active Directory e ativação de autenticação de multiplos fatores do Segura®. Uma vez cadastrado no AD, no grupo correspondente, o usuário ganham acesso ao PAM com o perfil correspondente à sua função.

Isso facilitou o uso diário, a gerência e incrementou segurança aos acessos privilegiados.

## COFRE DE SENHAS E DISPOSITIVOS

Um ponto alto da adoção do Segura® PAM foi a facilidade de integração dos dispositivos e credenciais na solução. A importação inicial por planilha trouxe os dispositivos, usuários e senhas.




Após a importação inicial, foi configurado o discovery periódico, para encontrar novos dispositivos, credenciais e chaves criptográficas, garantindo que não haverá mais credenciais privilegiadas sem a gestão da equipe da FIEMA.

A gestão e rotação de senhas mantém todas as senhas com alto nível de complexidade e eliminou a preocupação do time em decorar senhas ou anotá-las em blocos de notas ou cofres pessoais.

# GESTÃO DE SESSÕES

A gestão de sessões surpreendeu positivamente todo o time de TI. O primeiro benefício foi o acesso remoto por intermédio dos protocolos padrões (RPD, SSH, HTTPS, DATABASE), sem a necessidade de agentes e com possibilidade de utilizar os clientes de acesso remoto que o time já estava acostumado. Isso facilitou a adoção e simpificou o acesso.

A visualização de sessão em tempo real possibilita que as atividade sejam supervisionadas, mesmo quando a equipe não está trabalhando em um mesmo ambiente.

A gravação de sessão auxilia tanto em auditorias de acesso, quanto em registro das ações executadas nos dispositivos, para que sejam replicadas posteriormente.

# RASTREABILIDADE

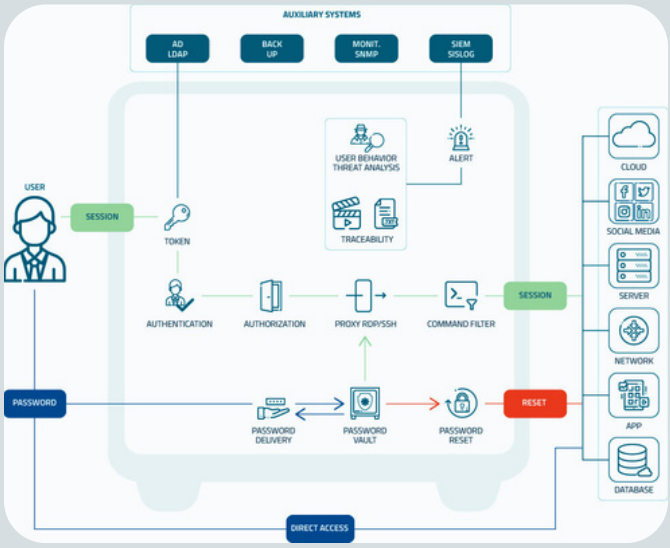
Além da rastreabilidade dos saques de senhas e acessos remotos, o Segura® permite dois outros tipos de controles que surpreenderam positivamente:

**1. Análise de comportamento do usuário**

É possível verificar de forma centralizada acessos que fogem do padrão de cada analista.

**2. Rastreabilidade na gestão**

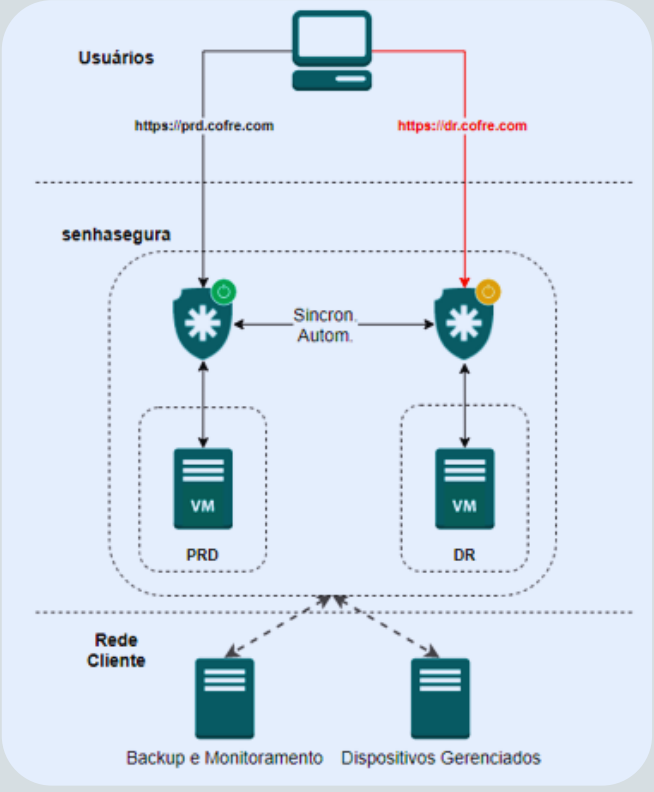
Todas as interações de gestão no Segura®, desde a visualização de logs, até a criação de dispositivos, são gravadas, trazendo possibilidade de auditoria. Isso traz segurança, pois não é possível, nem mesmo ao administrador da solução, burlar políticas de segurança da FIEMA.




# BACKUP E ALTA-DISPONIBILIDADE

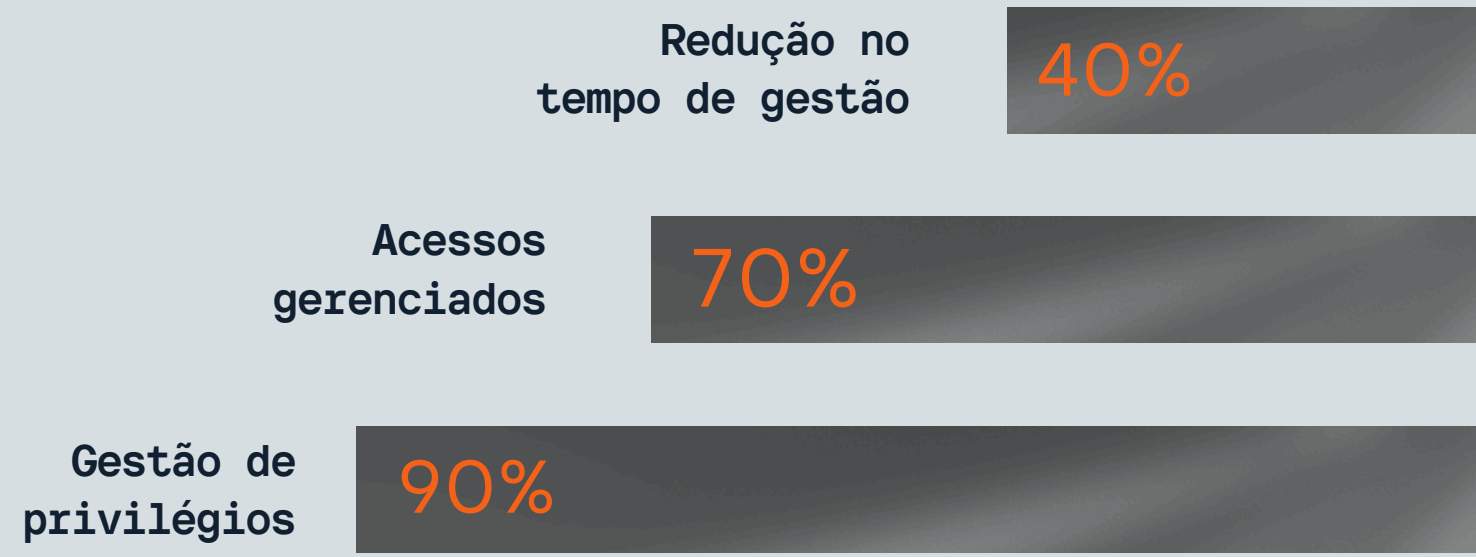
Uma das preocupações da FIEMA era o que ocorreria com a indisponibilidade do PAM.

Esse risco foi mitigado com alta-disponibilidade nativa e backup diário das credenciais, log e gravações.



# RESULTADOS

Melhoria na segurança dos acessos privilegiados, redução dos riscos de erros operacionais e vazamentos de senhas e gerenciamento de privilégios eficiente e auditável.




Com a adoção do Segura® PAM a FIEMA conseguiu em média:

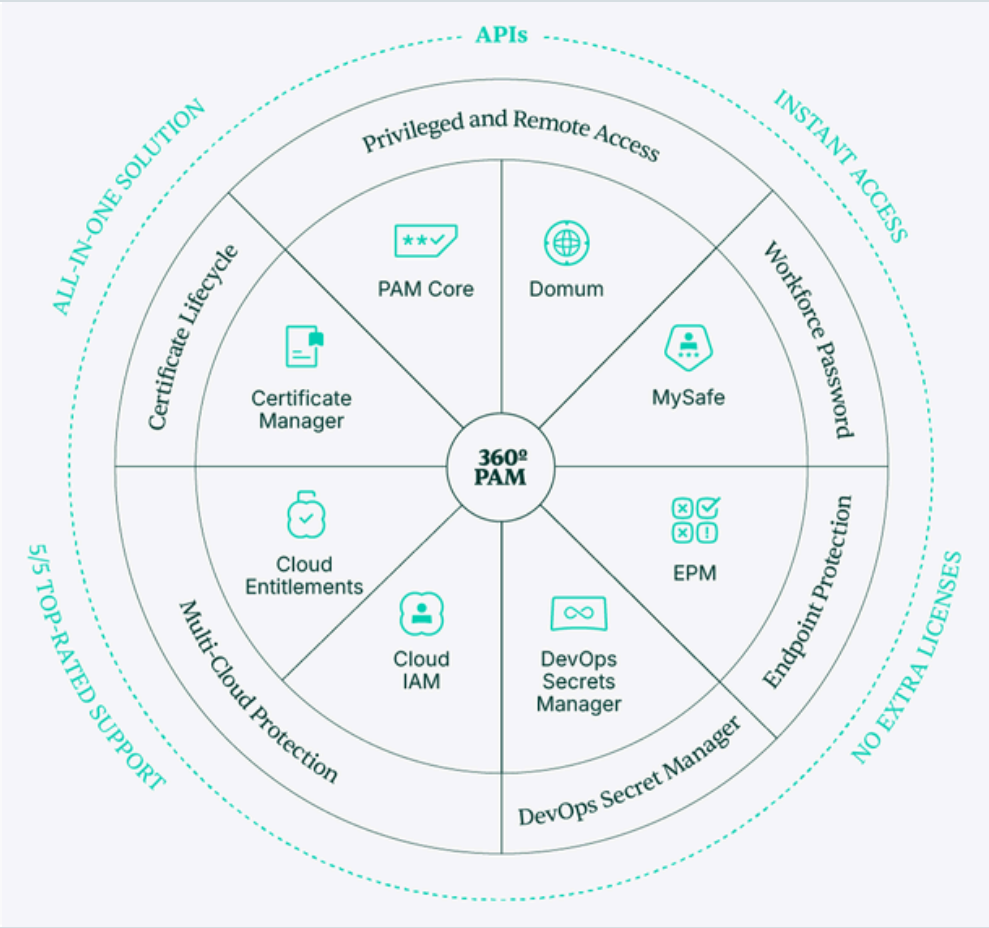
- Reduzir em 40% (quarenta por cento o tempo gasto com criação de senhas, grupos do AD, gestão de privilégios e controles de acesso, liberando tempo do time para outras atividades.
- Gerenciar 70% (setenta por cento) dos acessos privilegiados, restando os acessos remotos e acessos de aplicativos..
- Atingir 90% (noventa por cento) da meta de gestão de acesso privilegiado, gerenciando todo o acesso humano da equipe interna da FIEMA.

# PRÓXIMOS PASSOS

A FIEMA tem como próximos passos avançar na gestão de privilégios, implantando as demais soluções registradas na Ata de Registro de Preços.

Por ordem de prioridade, foi elencado como próximos passos:

- Gestão de acessos remotos
- Gestão de senhas para toda a organização
- Gestão de elevação de privilégios
- Gestão de senhas em aplicações
- Gestão de certificados digitais




"O fortalecimento da postura de cibersegurança é uma jornada que não tem data de finalização, pois novas ameaças sugem a cada momento. **Nós, da ITware, nos sentimos privilegiados** em fazer parte dessa jornada com a **FIEMA**, entregando uma solução líder de mercado - **Segura®** - e dedicando nossos esforços não apenas na implantação da solução, mas apoiando a adoção e o aumento na maturidade em cibersegurança."

**MARCOS SIQUEIRA - DIRETOR DE SOLUÇÕES DA ITWARE**

# OPINIÃO DOS USUÁRIOS

"A solução trouxe um nível de visibilidade e controle que antes não tínhamos, permitindo identificar e mitigar riscos rapidamente."

Fábio Feitosa, Coordenador de TI

"Acesso centralizado às credenciais reduziu significativamente o tempo gasto em tarefas administrativas, permitindo-nos focar em projetos mais estratégicos."

**RENAN COSTA, ANALISTA DE TI**

"O Segura facilitou o cumprimento das normas regulatórias, proporcionando auditorias mais tranquilas e seguras."

**CARLOS PEREIRA, ANALISTA DE TI**

# CASO DE SUCESSO

Nossa missão é projetar e implantar soluções em Tecnologia da Informação que otimizem e protejam os negócios de nossos clientes.

itware

## CONTATOS

www.itware.com.br
contato@itware.com.br