EBOOK

# GESTÃO DE ACESSO PRIVILEGIADO 101

segura®

# Sobre este eBook

No mundo digital em rápida evolução de hoje, as organizações enfrentam uma gama cada vez maior de ameaças de segurança cibernética que podem comprometer sistemas críticos, dados confidenciais e operações de negócio.

Com estatísticas alarmantes, como 63% das violações envolvem credenciais de dados (Relatório 2022 Verizon Data Breach Investigations) e 80% das violações de segurança envolvendo credenciais privilegiadas (Forrester Research), Gestão de Acesso Privilegiados (PAM) tornou-se um componente indispensável de uma estratégia abrangente de segurança cibernética.

“Gestão de Acessos Privilegiados 101 - Uma Introdução Compreensiva sobre PAM” é uma leitura obrigatória para quem busca reforçar a postura de segurança de sua organização e se proteger contra o espectro crescente de ameaças cibernéticas.

Este eBook foi desenvolvido para fornecer a você um entendimento aprofundado sobre PAM, sua importância no cenário atual de segurança cibernética e etapas práticas para implementar uma solução PAM de forma bem-sucedida.

**Não espere que ocorra um incidente cibernético antes de reconhecer a importância de PAM. Equipe-se com o conhecimento e as ferramentas necessárias para proteger os ativos mais críticos da sua organização mergulhando neste guia abrangente.**

# Índice

EBOOK

GESTÃO DE ACESSO PRIVILEGIADO 101

Capítulo 1

# Introdução ao Gerenciamento de Acesso Privilegiado

# O que é Gerenciamento de Acesso Privilegiado?

Na era digital, as organizações dependem muito da tecnologia para conduzir suas operações, manter dados sensíveis e dar suporte a sistemas críticos. Como resultado,proteger esses recursos se torna uma prioridade máxima. O Gerenciamento de Acesso Privilegiado, ou PAM, é uma solução de cibersegurança projetada para proteger os ativos digitais mais valiosos de uma organização, controlando e monitorando o acesso privilegiado a sistemas críticos e dados sensíveis.

O PAM garante que apenas usuários autorizados tenham acesso aos sistemas e informações que precisam para desempenhar suas funções. Ao implementar uma solução PAM, as organizações podem minimizar o risco de violações de dados, ameaças internas e outros incidentes de segurança cibernética que possam comprometer a integridade de seus sistemas e dados.

**63%**

63% das violações envolveram dados de credenciais.[1]

**$4.35M**

Custo médio global de uma violação de dados é de US$ 4,35 milhões.[2]

**74%**

Das empresas que implementam totalmente tecnologias de automação de segurança, incluindo PAM, experimentam cerca de 74% menor custo de violação de dados em comparação com aquelas que não têm essas tecnologias implantadas.[3]

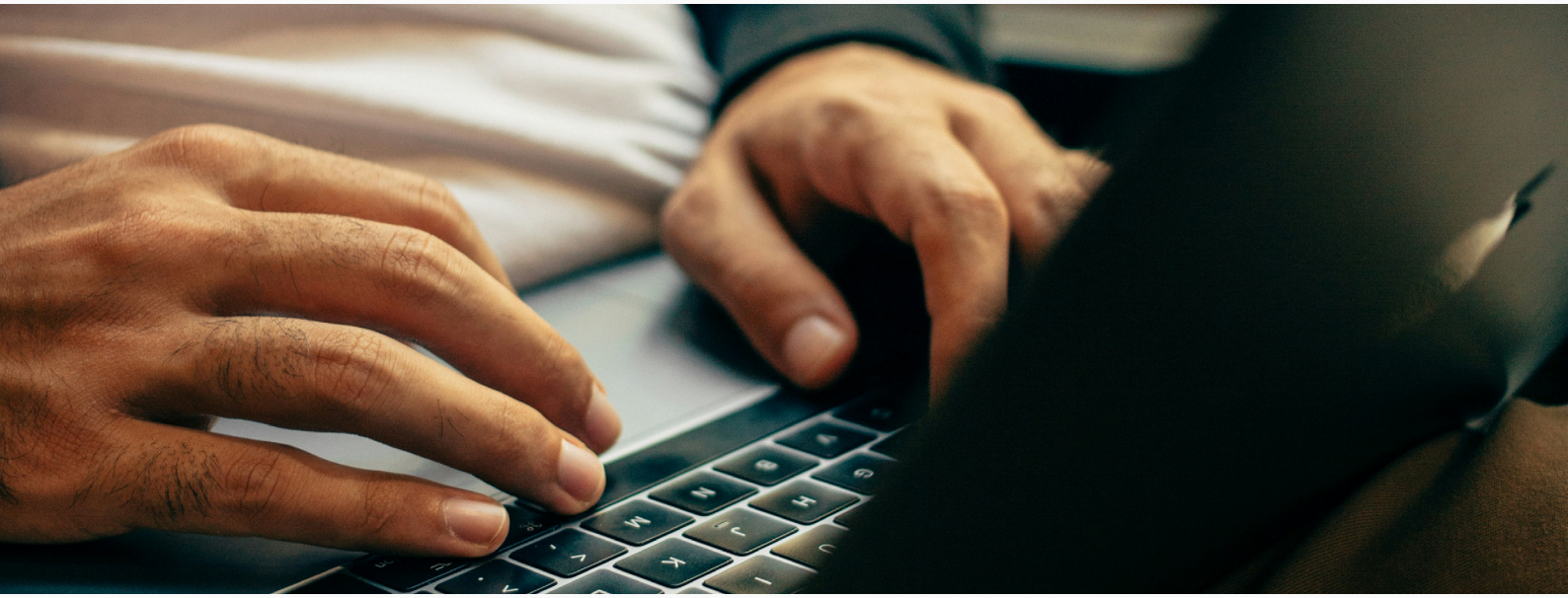
[1] Relatório de investigações de violação de dados da Verizon de 2022.
[2] IBM | Custo de uma violação de dados de 2022.
[3] Relatório de custo de violação de dados do Ponemon Institute de 2020.

# Por que PAM é importante?

Usuários privilegiados, como administradores de sistemas, executivos e fornecedores terceirizados, têm acesso às informações e recursos mais sensíveis de uma organização. Esse acesso privilegiado, se não gerenciado corretamente, pode levar a acesso não autorizado, violações de dados e outros incidentes de segurança cibernética que podem ter consequências devastadoras para a organização.

## O PAM é essencial para as organizações:

- Garantir que apenas usuários autorizados tenham acesso a informações sensíveis e sistemas críticos.
- Monitorar e controlar a atividade de usuários privilegiados para evitar acesso não autorizado e detectar ameaças potenciais em tempo real.
- Manter a conformidade com regulamentos e padrões da indústria, como GDPR,HIPAA e PCI DSS.
- Melhorar a postura geral de segurança cibernética, reduzindo a superfície de ataque e limitando o potencial de ameaças internas ou ataques externos.



# Principais componentes de uma solução PAM

Uma solução PAM abrangente deve incluir os seguintes componentes principais:

### Gerenciamento de acesso

Controle quem tem acesso a quais recursos, sistemas e dados,implementando controles de acesso baseados em função, autenticação multifator e fornecimento de acesso sob demanda.

### Gerenciamento de credenciais

Armazene, gerencie e rotacione com segurança as credenciais de contas privilegiadas, como senhas e chaves, para evitar acesso não autorizado e reduzir o risco de roubo ou mau uso de credenciais.

### Gerenciamento de sessões

Monitore e registre sessões de usuários privilegiados em tempo real, permitindo a detecção de atividades suspeitas, auditoria das ações realizadas e a capacidade de encerrar sessões, se necessário.

### Análise de usuário privilegiado

Analise o comportamento do usuário e identifique potenciais riscos de segurança por meio do uso de técnicas de inteligência artificial e aprendizado de máquina. Isso permite que as organizações detectem e respondam a possíveis ameaças mais rapidamente.

### Auditoria e conformidade

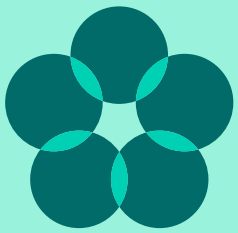
Acompanhe e relate as atividades de usuários privilegiados para garantir a conformidade com políticas internas e regulamentos externos, além de fornecer uma trilha de auditoria clara para investigações forenses.

# Desafios na implementação de uma solução PAM

Embora o PAM seja um componente crítico da estratégia de cibersegurança de uma organização, a implementação de uma solução PAM pode ser desafiadora devido a vários fatores:

- Ambientes de TI complexos com inúmeros sistemas, aplicativos e dispositivos que exigem acesso privilegiado.
- Resistência dos usuários, que podem perceber o PAM como uma limitação à sua liberdade e flexibilidade.
- Restrições orçamentárias e dificuldade em justificar o investimento em PAM aos tomadores de decisão.
- Falta de conhecimento e expertise em tecnologias e melhores práticas de PAM.

**Apesar desses desafios, os benefícios da implementação de uma solução PAM superam em muito os riscos e custos potenciais associados à falta de uma solução em vigor.**



Nos próximos capítulos, exploraremos o papel crítico do PAM no cenário atual de cibersegurança, forneceremos um guia passo a passo para implementar uma solução PAM, apresentaremos a plataforma PAM da Segura® e seus recursos avançados de segurança e compartilharemos histórias de sucesso do mundo real de organizações que alcançaram segurança aprimorada com o PAM.

EBOOK

GESTÃO DE ACESSO PRIVILEGIADO 101

Capítulo 2

# O Papel Crítico do PAM na Cibersegurança Atual

# A Evolução do Cenário de Ameaças

O cenário de cibersegurança está em constante evolução, com os criminosos cibernéticos se tornando mais sofisticados e persistentes em seus ataques. As organizações enfrentam uma série de ameaças, incluindo:

- **Ameaças externas:** criminosos cibernéticos e atores estatais em busca de vulnerabilidades para explorar, roubar informações confidenciais ou interromper operações.
- **Ameaças internas:** funcionários, contratados ou parceiros descontentes que usam seu acesso privilegiado para comprometer sistemas ou dados.
- **Ameaças acidentais:** usuários bem-intencionados que inadvertidamente expõem a organização a riscos por meio de erros humanos ou práticas de segurança inadequadas.

Neste mundo interconectado, essas ameaças podem ter consequências de longo alcance para a reputação, estabilidade financeira e conformidade regulatória de uma organização.

> **Os cibercriminosos estão se tornando mais sofisticados e persistentes em seus ataques.**

# A Importância do PAM no Ecossistema de Cibersegurança

Dada a natureza complexa e em constante evolução das ameaças de cibersegurança, as organizações devem adotar uma abordagem de segurança em camadas para proteger seus ativos críticos. O PAM desempenha um papel crítico nesse ecossistema, ao:

### Minimizar a superfície de ataque

Ao limitar e controlar o acesso privilegiado, as organizações podem reduzir o número de pontos de entrada potenciais para os atacantes.

### Prevenir acesso não autorizado

O PAM garante que apenas os usuários certos tenham acesso aos recursos certos no momento certo, reduzindo significativamente o risco de acesso não autorizado.

### Detectar e responder a ameaças

Monitorar e analisar o comportamento do usuário privilegiado permite que as organizações identifiquem ameaças potenciais em tempo real e respondam adequadamente.

### Atender aos requisitos de conformidade

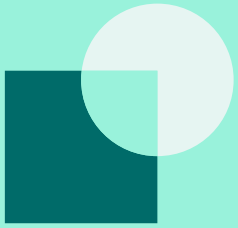
O PAM ajuda as organizações a manter a conformidade com várias regulamentações e padrões do setor, fornecendo trilhas de auditoria claras e aplicando controles de acesso.

# Integrando o PAM com outras soluções de segurança

Uma solução PAM robusta não deve operar isoladamente, mas sim ser integrada a outras soluções de segurança para fornecer proteção abrangente. As principais integrações incluem:

- **Gerenciamento de Identidade e Acesso (IAM):** o PAM trabalha em conjunto com o IAM para garantir que todos os usuários, não apenas os privilegiados, tenham o nível apropriado de acesso aos recursos.
- **Gerenciamento de Informações e Eventos de Segurança (SIEM):** alimentando dados de atividade do usuário privilegiado em uma solução SIEM, as organizações podem obter insights mais profundos sobre possíveis ameaças e melhorar sua postura de segurança geral.
- **Detecção e Resposta de Endpoint (EDR):** integrar o PAM com soluções EDR permite que as organizações monitorem e protejam endpoints onde usuários privilegiados acessa, sistemas e dados críticos.
- **Autenticação de múltiplos fatores (MFA):** combinando o PAM com o MFA adiciona uma camada extra de segurança, garantindo que os usuários devem fornecer várias formas de verificação antes de obter acesso a recursos privilegiados.

**Ao integrar o PAM com outras soluções de segurança, as organizações podem estabelecer uma estratégia de segurança abrangente e em camadas que aborda todo o espectro de ameaças cibernéticas.**



No próximo capítulo, forneceremos um guia passo a passo para implementar uma solução PAM, garantindo que sua organização esteja bem equipada para proteger seus sistemas críticos e dados sensíveis do cenário de ameaças em constante evolução.

EBOOK

GESTÃO DE ACESSO PRIVILEGIADO 101

Capítulo 3

# Guia passo a passo para implementar uma solução PAM

**Implementar uma solução PAM requer planejamento cuidadoso, execução e melhoria contínua. Este capítulo descreve um guia passo a passo para ajudar as organizações a implementar com sucesso uma solução PAM.**

# Avalie seu estado atual

Antes de implementar uma solução PAM, é essencial avaliar a postura de segurança atual de sua organização. Essa avaliação deve incluir:

1. Identificar todas as contas, usuários e sistemas privilegiados dentro da organização.

2. Avaliar os controles de acesso existentes, as práticas de gerenciamento de senhas e as capacidades de monitoramento.

3. Identificar lacunas e áreas de melhoria em sua estratégia atual de gerenciamento de acesso privilegiado.

# Defina sua estratégia de PAM

Com base na avaliação, desenvolva uma estratégia de PAM que aborde as lacunas identificadas e esteja alinhada com os objetivos gerais de segurança de sua organização. Os principais elementos da estratégia devem incluir:

1. Estabelecer metas e objetivos claros para sua implementação de PAM.

2. Definir funções e responsabilidades para a administração e supervisão do PAM.

3. Desenvolver políticas e procedimentos para o gerenciamento de acesso privilegiado, incluindo processos de solicitação, aprovação e revisão de acesso.

# Selecione a solução PAM correta

Escolha uma solução PAM que atenda às necessidades de sua organização e integre-se perfeitamente à sua infraestrutura de segurança existente. Considere fatores como:

1. Compatibilidade com seu ambiente de TI e soluções de segurança existentes.

2. Escalabilidade e flexibilidade para se adaptar ao crescimento e mudanças futuras.

3. Facilidade de implantação e gerenciamento contínuo.

4. Reputação, suporte e expertise do fornecedor.

# Implante a solução PAM

Depois de selecionar a solução PAM correta, siga estas etapas para uma implantação bem-sucedida:

1. Planeje e comunique: Comunique claramente as metas, objetivos e prazos da implementação de PAM para todas as partes interessadas.

2. Configure e personalize: Configure a solução PAM para se alinhar com as políticas, procedimentos e ambiente de TI de sua organização. Personalize a solução para atender às suas necessidades e requisitos específicos.

3. Treine e eduque: Treine administradores e usuários finais sobre como usar a solução PAM de forma eficaz. Eduque os usuários sobre a importância do gerenciamento de acesso privilegiado e seu papel na manutenção da segurança.

# Monitorar, revisar e melhorar

Implementar uma solução de PAM não é um evento único, mas um processo contínuo. Monitore, revise e melhore continuamente sua estratégia de PAM:

1. Revisando regularmente os direitos e privilégios de acesso para garantir que permaneçam apropriados e atualizados.
2. Monitorando a atividade do usuário privilegiado e analisando padrões comportamentais para identificar ameaças potenciais.
3. Realizando auditorias e avaliações periódicas para garantir conformidade com políticas internas e regulamentações externas.
4. Atualizando e refinando sua estratégia de PAM à medida que sua organização evolui e novas ameaças surgem.

**Seguindo esses passos, sua organização pode implementar com sucesso uma solução de PAM que fortalece sua postura de cibersegurança e protege seus ativos mais críticos.**

No próximo capítulo, apresentaremos a plataforma de PAM da Segura® e seus recursos avançados de segurança que podem ajudar sua organização a alcançar uma segurança e conformidade aprimoradas.

EBOOK

GESTÃO DE ACESSO PRIVILEGIADO 101

Capítulo 4

# Desbloqueando o Poder dos Recursos Avançados de Segurança

# Desbloqueando o Poder dos Recursos Avançados de Segurança

A plataforma PAM da Segura® oferece uma solução abrangente e inovadora projetada para abordar os desafios do gerenciamento de acesso privilegiado no cenário complexo e em constante evolução da cibersegurança atual.

Este capítulo irá apresentá-lo aos recursos avançados de segurança que diferenciam a plataforma PAM da Segura® de outras soluções do mercado.

## Gerenciamento de Acesso

A plataforma PAM da Segura oferece recursos robustos de gerenciamento de acesso, incluindo:

- Controle de Acesso Baseado em Função (RBAC): Atribua direitos de acesso com base em funções predefinidas, garantindo que os usuários tenham o nível apropriado de acesso para realizar suas funções.
- Acesso Just-In-Time (JITA): Conceda acesso temporário e limitado a recursos privilegiados, reduzindo o risco de acesso ou uso não autorizado.
- Autenticação Multifator (MFA): Exija que os usuários forneçam várias formas de verificação antes de obter acesso a recursos privilegiados, adicionando uma camada extra de segurança.

## Gerenciamento de Credenciais

A plataforma PAM da Segura oferece recursos avançados de gerenciamento de credenciais, como:

- Cofre de Senhas Seguro: Armazene, gerencie e rotacione as credenciais privilegiadas em um repositório centralizado e criptografado, impedindo o acesso não autorizado e reduzindo o risco de roubo ou uso indevido de credenciais.
- Rotação Automática de Senhas: Roteacione automaticamente senhas e chaves de contas privilegiadas em intervalos predefinidos ou com base em eventos específicos, garantindo que as credenciais permaneçam seguras e atualizadas.
- Gravação e Reprodução de Sessão: Grave todas as sessões de usuário privilegiado para fins de auditoria e conformidade e habilite a reprodução para revisar ações do usuário e identificar potenciais riscos de segurança.

## Gerenciamento e Monitoramento de Sessão

Monitore e controle as sessões de usuário privilegiado em tempo real com a plataforma PAM da Segura®:

- Monitoramento de Sessão em Tempo Real: Veja as sessões de usuário privilegiado em tempo real, detecte atividades suspeitas e tome medidas imediatas, como terminar sessões ou revogar o acesso.
- Isolamento de Sessão e Proxy de Usuário Privilegiado: Isole sessões de usuário privilegiado de sistemas críticos e use um proxy para garantir que os usuários nunca acessem recursos privilegiados diretamente, reduzindo o risco de propagação de malware ou roubo de credenciais.
- Controle de Acesso Granular: Imponha controles de acesso granulares, como permitir ou negar comandos específicos, impedindo que os usuários executem ações não autorizadas durante sessões privilegiadas.

---

## Análise de Usuário Privilegiado

A plataforma PAM da Segura utiliza inteligência artificial e aprendizado de máquina para fornecer análises avançadas de usuário privilegiado:

- Análise de Comportamento do Usuário (UBA): Analise o comportamento do usuário privilegiado para identificar padrões e anomalias, permitindo que as organizações detectem e respondam a possíveis ameaças com mais rapidez.
- Pontuação de Risco: Atribua pontuações de risco aos usuários privilegiados com base em seu comportamento, padrões de acesso e outros fatores, permitindo que as organizações priorizem os esforços de monitoramento e resposta.

---

## Auditoria e Conformidade

Mantenha a conformidade e forneça trilhas de auditoria claras com a plataforma PAM da Segura®:

- Relatórios Abrangentes: Gere relatórios detalhados sobre atividades de usuários privilegiados, direitos de acesso, alterações de senhas e muito mais, garantindo a conformidade com políticas internas e regulamentações externas.
- Painéis Personalizáveis: Crie painéis personalizáveis para visualizar métricas importantes de PAM e obter insights sobre a postura de segurança da sua organização.

**Ao aproveitar os recursos avançados de segurança da plataforma PAM da Segura®, as organizações podem alcançar segurança aprimorada, conformidade e eficiência operacional na gestão de acesso privilegiado.**

No próximo capítulo, compartilharemos histórias de sucesso do mundo real de organizações que transformaram sua postura de segurança por meio da implementação da solução PAM da Segura®.

EBOOK

GESTÃO DE ACESSO PRIVILEGIADO 101

Capítulo 5

# Histórias de sucesso do mundo real: Como as organizações alcançaram segurança aprimorada com PAM

# Como as organizações alcançaram segurança aprimorada com PAM

## Instituição Financeira: Fortalecendo a Conformidade e Reduzindo Ameaças Internas

Uma grande instituição financeira enfrentou desafios para atender aos requisitos de conformidade regulatória e gerenciar o risco de ameaças internas. Ao implementar a plataforma PAM da Segura®, a organização conseguiu:

- Centralizar e automatizar o gerenciamento de acesso privilegiado, reduzindo o risco de acesso não autorizado e ameaças internas.
- Aplicar controles de acesso baseados em funções e autenticação de múltiplos fatores, garantindo que apenas usuários autorizados tenham acesso a sistemas e dados sensíveis.
- Agilizar os processos de relatórios e auditorias de conformidade, economizando tempo e recursos enquanto mantém a aderência às regulamentações do setor.

O resultado foi um ambiente mais seguro e em conformidade, com risco reduzido de violações de dados e ameaças internas, juntamente com uma melhoria na eficiência operacional.

## Organização de Saúde: Protegendo Dados Sensíveis do Paciente e Garantindo a Conformidade com o HIPAA

Uma grande organização de saúde precisava proteger dados sensíveis de pacientes e garantir a conformidade com a Lei de Portabilidade e Responsabilidade do Seguro de Saúde (HIPAA). A implementação da solução PAM da Segura® permitiu à organização:

- Garantir a segurança e o gerenciamento de credenciais privilegiadas, evitando acesso não autorizado a dados de pacientes e sistemas críticos.
- Monitorar e registrar as sessões de usuários privilegiados, fornecendo um histórico de auditoria para conformidade e investigações forenses.
- Detectar e responder a possíveis ameaças em tempo real por meio de análises avançadas de comportamento do usuário.
- A organização de saúde obteve uma segurança aprimorada, garantindo a confidencialidade e a integridade dos dados do paciente enquanto mantém a conformidade com o HIPAA.

## Empresa de Manufatura: Segurança nas Operações Globais e Redução da Superfície de Ataque

Uma empresa de manufatura global com uma infraestrutura de TI complexa buscou melhorar sua postura de segurança e reduzir a superfície de ataque potencial. Com a plataforma PAM da Segura®, a empresa foi capaz de:

- Obter visibilidade e controle sobre todas as contas, usuários e sistemas privilegiados em toda a empresa.
- Implementar acesso just-in-time e rotação automática de senhas, reduzindo o risco de acesso não autorizado e roubo de credenciais.
- Integrar PAM com soluções de segurança existentes, como SIEM e EDR, para criar uma estratégia de segurança abrangente e em várias camadas.

O resultado foi um ambiente mais seguro que reduziu a superfície de ataque e protegeu ossistemas e dados críticos da organização de possíveis ameaças.

Esses casos de sucesso ilustram o poder da solução PAM da Segura® em ajudar organizações de vários tamanhos e setores a alcançar uma segurança aprimorada, conformidade e eficiência operacional.

**Ao implementar uma estratégia sólida de Gestão de Acessos Privilegiados (PAM) e aproveitar os recursos avançados da plataforma PAM da Segura®, sua organização pode proteger efetivamente seus ativos mais valiosos no cenário complexo e em constante evolução da cibersegurança.**

EBOOK

GESTÃO DE ACESSO PRIVILEGIADO 101

Capítulo 6

# Conclusão

# Protegendo Sua Organização de Ransomware, Ameaças Internas e Ciberataques com o Gerenciamento de Acesso Privilegiado.

No mundo digital de hoje, as organizações enfrentam um número cada vez maior de ameaças cibernéticas, incluindo ataques de ransomware, ameaças internas e ciberataques direcionados de adversários externos. Para proteger efetivamente os sistemas críticos e dados sensíveis de sua organização, é essencial implementar uma estratégia abrangente de cibersegurança.

Um componente-chave desta estratégia é o Gerenciamento de Acesso Privilegiado (PAM), que oferece controles de acesso robustos, capacidades de monitoramento e medidas preventivas para impedir o acesso não autorizado e manter a conformidade com as regulamentações do setor.

Neste eBook, examinamos a importância do PAM, fornecemos um guia passo a passo para implementar uma solução PAM e mostramos os recursos avançados de segurança da plataforma PAM da Segura®.

**Seguindo essas diretrizes e aproveitando o poder da solução PAM inovadora da Segura®, sua organização pode fortalecer suas defesas contra ransomware, mitigar ameaças internas e evitar que ciberataques comprometam seus ativos críticos.**

# Agende uma demonstração

Não deixe a segurança de sua organização vulnerável a ransomware, ameaças internas e atacantes externos. Invista em uma solução robusta de PAM que fortalecerá suas  efesas e ajudará sua organização a prosperar diante de desafios de cibersegurança em constante evolução. Agende uma demonstração da plataforma PAM da Segura® hoje e  descubra como nossos recursos avançados de segurança podem revolucionar a postura de segurança de sua organização.

Para agendar uma demonstração, clique aqui e preencha o formulário de solicitação de demonstração. Nossa equipe de especialistas ficará feliz em demonstrar como a plataforma PAM da Segura® pode atender efetivamente às necessidades de segurança exclusivasde sua organização e ajudá-lo a alcançar seus objetivos de cibersegurança.

## Pronto para elevar a segurança cibernética de sua organização?

Descubra as soluções de ponta da Segura® para proteger dados sensíveis e sistemas críticos contra ameaças cibernéticas.

**SOLICITE UMA DEMONSTRAÇÃO AGORA**

**Segura®: Futureproof Identity Security.**

A Segura® é líder em Privileged Access Management (PAM), entregando às equipes de TI uma solução rápida e fácil de usar, sem complexidade na implementação. Simplificamos o gerenciamento de acessos privilegiados com uma plataforma intuitiva, escalável e pensada para o dia a dia real das equipes.

Nossa inovação, robustez e experiência do cliente foram reconhecidas globalmente por Gartner, KuppingerCole e Frost & Sullivan. Além disso, somos classificados como solução PAM nº 1 por usuários reais no Gartner Peer Insights.

Com implantação ágil, automação precisa e zero custos ocultos, a Segura® é segurança que trabalha por você—simples assim.

segura®

EBOOK

# GESTÃO DE ACESSO PRIVILEGIADO 101


**Document Classification: Public | February 2025**