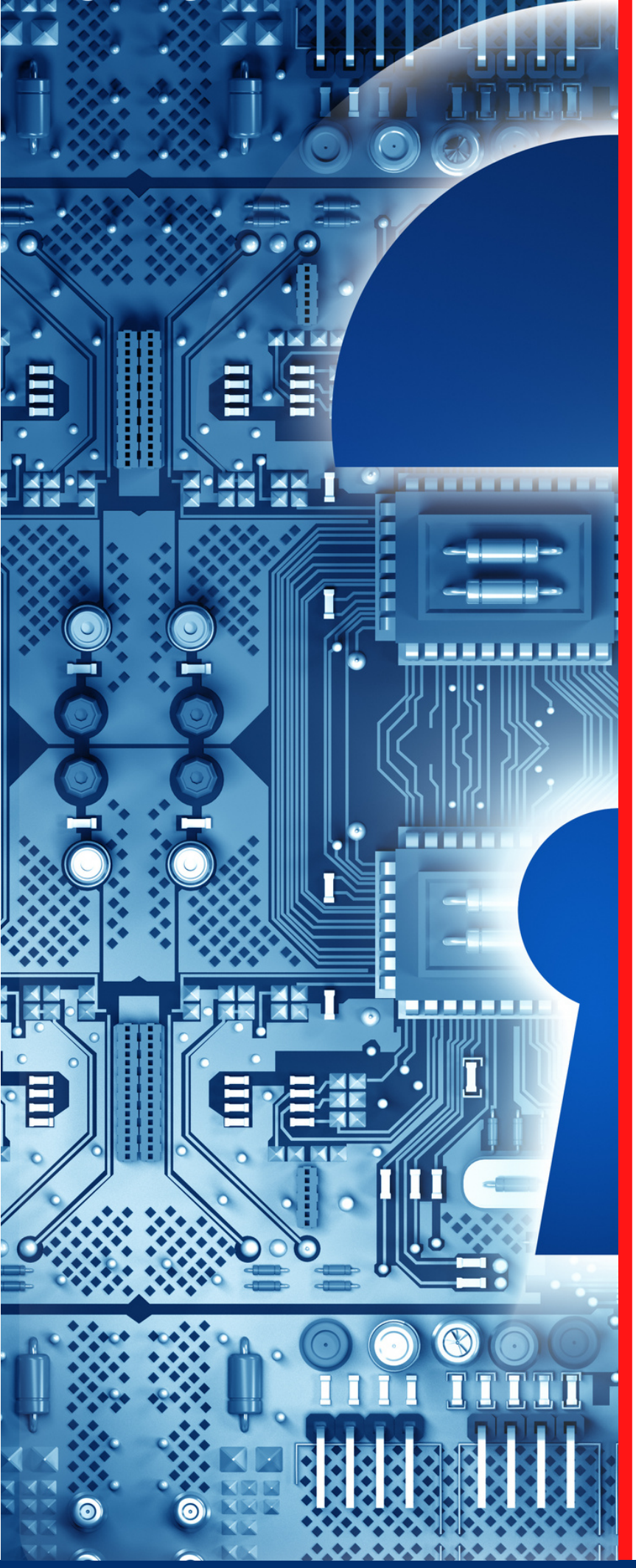


OSIC

ORIENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

08/2023

Gestão de Acesso Privilegiado

(*Privileged Access Management* – PAM)

Parte 1 de 2

Textos: João Alberto Muniz Gaspar
Diagramação: Douglas Rocha de Oliveira
Produção: Secretaria de Segurança da Informação e Cibernética

Espaço cibernético inclusivo, seguro, estável, acessível e pacífico.

TLP:CLEAR

Introdução

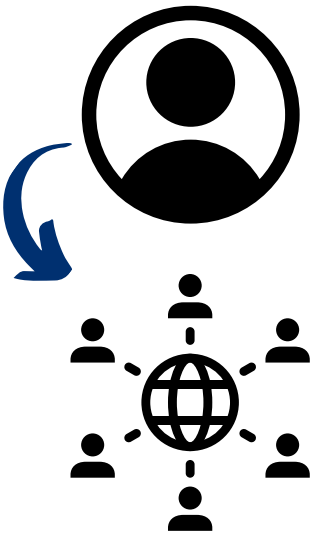
Contas com privilégios, particularmente de administrador, são as favoritas entre os invasores que buscam obter acesso a servidores de dados sensiveis sem atrair suspeitas. Os invasores utilizam diversos métodos (como *phishing*, engenharia social, etc.) para obter de usuários válidos suas informações de *login* e até suas senhas de forma a obter acesso a um sistema. Uma vez dentro do sistema, os invasores imediatamente procuram por credenciais privilegiadas não gerenciadas de forma a escalar seus privilégios, preferencialmente para o status de administrador de domínio, a fim de conseguir acesso irrestrito aos recursos disponíveis.

Da mesma forma, usuários internos com contas privilegiadas, mal-intencionados podem causar mais danos do que terceiros. A confiança inerente depositada nos chamados "*insiders*" permite que eles aproveitem seus privilégios de usuário existentes para exfiltrar dados e oferecer para terceiros em troca de benefícios, normalmente financeiros, sem que a organização perceba.

Em face da importância e da complexidade, a Gestão de Acesso Privilegiado ou, na sigla em inglês, PAM, será tratada em duas edições da Orientação de Segurança da Informação e Cibernética (OSIC). Nesta primeira edição, trataremos da parte mais conceitual do tema.

Privilégio, contas privilegiadas e credenciais privilegiadas

No contexto da tecnologia da informação, **privilégio** pode ser definido como o nível de autoridade de uma determinada conta ou processo dentro de uma rede ou de um sistema de computação. Certos graus de privilégio podem permitir que determinado usuário possa ignorar ou se sobrepor a determinadas restrições de segurança, podendo incluir permissões para executar ações como finalizar processos, instalar dispositivos, configurar ativos ou sistemas, etc. Portanto, ser um usuário com privilégios é uma vantagem ou direito especial, uma elevação em relação às restrições normalmente aplicadas aos usuários comuns.



Estabelecer níveis de privilégio também serve a diversos propósitos operacionais ao conceder direitos elevados a determinados usuários, aplicações ou outros processos do sistema de forma que eles possam acessar recursos e executar tarefas sensíveis ao sistema. Por esses motivos, contas privilegiadas são alvos prioritários para os invasores.

CONTA PRIVILEGIADA

Como regra geral, a maioria dos usuários deveria operar com contas não-privilegiadas na maioria do tempo. Contas não-privilegiadas, também chamadas de Contas de Privilégio Mínimo (*Least-privilege User Account* – LUA), são geralmente de dois tipos:

- **contas de usuário padrão:** possuem um conjunto bem limitado de privilégios de forma a acessar apenas os recursos estritamente necessários ao cumprimento das atividades rotineiras; e
- **contas de convidado:** possuem privilégios ainda menores do que as contas de usuário padrão, geralmente restritas a aplicações básicas e navegação na *internet*.

Uma conta privilegiada é considerada qualquer conta que fornece acesso e privilégios além dos previstos para as contas não-privilegiadas. Um usuário privilegiado é qualquer usuário ao qual foi concedido acesso privilegiado a recursos através de uma conta privilegiada.

CONTAS DE SUPERUSUÁRIO

Contas de superusuário são um tipo especial de conta privilegiada, sendo utilizadas primariamente pelos administradores de rede e fornecem poder irrestrito para executar comandos e executar mudanças no sistema. Além disso, geralmente, os privilégios da conta de superusuário garantem acesso irrestrito aos recursos do sistema com poderes completos – ou seja, a capacidade de ler, executar, criar, alterar e excluir arquivos, diretórios, contas de outros usuários, configurações do sistema e *drivers* de dispositivos, dentre outros. Isso torna a conta de superusuário um alvo extremamente vantajoso para os invasores.

Outro aspecto a ser ressaltado é que contas privilegiadas também podem se referir a contas de usuários não humanos, quando as contas são associadas a uma identidade de máquina e não a uma pessoa. As contas privilegiadas associadas a uma identidade de máquina mais comuns são:

- **conta de administrador padrão:** é uma conta não pessoal e, geralmente, é a primeira conta a ser criada durante a instalação de um sistema operacional. Ela simplesmente dá a qualquer usuário direitos completos sobre todo o sistema. O grande problema relativo a essa conta é que, muitas vezes, após a instalação do sistema e da criação de contas de usuários com privilégio de administração, ela acaba sendo esquecida, tornando-se o alvo perfeito para as ameaças que tenham como objetivo realizar uma invasão;

- **contas de serviço:** são normalmente usadas em sistemas operacionais para executar aplicativos ou programas, seja no contexto de contas do sistema (contas com privilégios altos e sem nenhuma senha) ou uma conta de usuário específica, geralmente criada manualmente ou durante a instalação do *software*. Geralmente não têm permissão para fazer *login* nos sistemas, mas têm senhas que nunca mudam nem expiram. Por esse motivo, são geralmente exploradas por invasores que encontram maneiras de quebrá-las para que possam executar seus próprios códigos de programa com privilégios elevados, permitindo acesso remoto ao invasor; e

- **contas de aplicativos:** são usadas frequentemente para garantir que um aplicativo tenha acesso aos recursos necessários para funcionar, como bancos de dados, rede, tarefas automatizadas (como implantação de *software*), atualizações automatizadas e a capacidade de fazer alterações na configuração. Essas contas geralmente mantêm senhas em arquivos de configuração ou às vezes usam contas locais ou de serviço para obter o acesso necessário. As contas de aplicativos também são um alvo para invasores, pois podem facilmente ser exploradas usando vulnerabilidades conhecidas, permitindo que invasores obtenham acesso remoto, modifiquem códigos do sistema ou elevem contas padrão para privilegiadas e possam se mover pela rede.

A proliferação de contas privilegiadas associadas à identidade de máquinas amplia a complexidade da segurança da informação no ambiente.

CREDENCIAIS PRIVILEGIADAS

Credenciais privilegiadas - também chamadas de “segredos”, especialmente em ambientes que adotem a cultura *DevOps*[1], são um subconjunto de credenciais usadas por usuários privilegiados para obter acesso elevado a contas, servidores, bancos de dados, aplicativos e outros sistemas sensíveis. Além das senhas, as credenciais privilegiadas também incluem segredos como chaves SSH[2], chaves API, *tokens* e certificados.

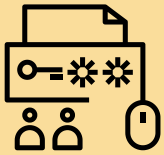
Credenciais privilegiadas usadas por contas de superusuário podem vir a fornecer acesso privilegiado ilimitado através dos sistemas e dados mais críticos de uma organização. Em função desse poder, elas são extremamente desejadas pelos invasores e podem ser abusadas por usuários internos mal-intencionados.

IAM X PAM X PIM

A Gestão de Acesso e Identidade (IAM) é um *framework* comumente utilizado por equipes de segurança e tecnologia da informação para gerenciar identidades, determinando quais pessoas terão acesso a certos recursos de uma organização, sejam eles redes, dispositivos ou bancos de dados, por exemplo. A IAM tem como principal objetivo facilitar a gestão de identidade dos usuários dentro de uma organização, garantindo que somente pessoas autorizadas tenham acesso aos recursos adequados para a sua função, seguindo as políticas de segurança da organização.

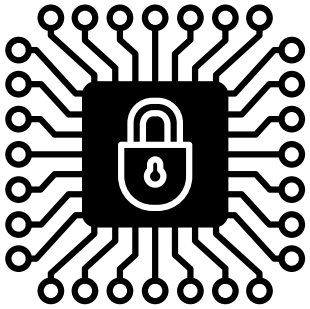
A Gestão de Identidade Privilegiada (PIM) é o processo que as organizações usam para gerenciar quais usuários privilegiados – incluindo usuários humanos e usuários máquinas (ou não-humanos) – têm acesso a quais recursos.
As políticas de segurança aplicadas pela PIM geralmente se concentram no controle de usuários com permissões elevadas para alterar configurações, provisionar ou retirar acesso e fazer outras alterações significativas sem supervisão formal. Algumas organizações usam soluções PIM para monitorar o comportamento do usuário e o acesso distribuído para evitar que os administradores tenham muitas permissões.

A Gestão de Acesso Privilegiado (PAM) e a Gestão de Identidade Privilegiada (PIM) são subconjuntos da IAM. A PAM e a PIM se concentram nos acessos privilegiados enquanto que a solução IAM trata do gerenciamento de senhas, autenticação multifator (MFA), *login* único (SSO) e gerenciamento do ciclo de vida do usuário para todos contas, não apenas aquelas com acesso privilegiado.

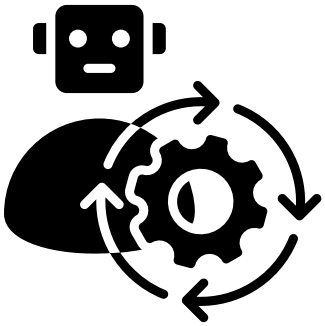


A Gestão de Acesso Privilegiado (PAM) é o processo de controlar e monitorar o acesso a recursos críticos da organização, geralmente usando tecnologias de gerenciamento de identidade e acesso.
A principal diferença entre PIM e PAM é que a PIM trata do acesso que já foi concedido ao usuário enquanto a PAM se preocupa em como monitorar e controlar o acesso sempre que um usuário solicitar acesso a um recurso.
A PIM se concentra na gestão de recursos e na definição de quais funções ou atributos determinam que um usuário obtenha acesso a recursos específicos. Já a PAM se concentra nas políticas e ferramentas de segurança que ajudam as organizações a armazenar e criptografar credenciais, validar se os usuários têm permissão para acessar determinados recursos e fornecer uma maneira segura para usuários aprovados acessarem sistemas, ferramentas e dados críticos.

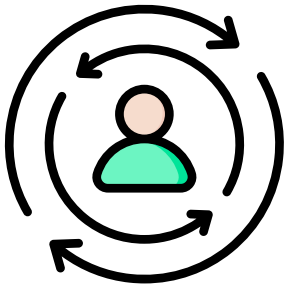
A Gestão de Acesso Privilegiado (PAM) e seus benefícios



A Gestão de Acesso Privilegiado (PAM) consiste nas estratégias e tecnologias de segurança cibernética para exercer controle sobre o acesso privilegiado e permissões para usuários, contas, processos e sistemas em um ambiente de TI. Ao dimensionar corretamente os controles de acesso privilegiado, o PAM ajuda as organizações a reduzir sua superfície de ataque e a prevenir, ou pelo menos mitigar, os danos decorrentes de ataques externos, bem como de má conduta ou negligência interna.



Uma solução PAM deve ter os recursos necessários para suportar as políticas de segurança de uma organização. Normalmente, uma PAM corporativa terá recursos automatizados de gerenciamento de senhas que incluem um cofre de senhas, rotação automática, geração automática e um fluxo de trabalho de aprovação. Além desses recursos de gerenciamento de credenciais, ela também deve fornecer aos administradores a capacidade de implementar e reforçar a autenticação multifator.



A solução PAM também deve oferecer às organizações a capacidade de gerenciar ciclos de vida de contas privilegiadas, ou seja, deve dar aos administradores a capacidade de automatizar a criação, a alteração e a exclusão de contas.

Por fim, como os agentes responsáveis pela segurança precisam monitorar constantemente as sessões privilegiadas e investigar quaisquer anomalias, a PAM deve fornecer mecanismos de monitoramento em tempo real com a geração de alertas automatizados e relatórios robustos.

Embora o gerenciamento de privilégios englobe muitas estratégias, um objetivo central é a imposição do privilégio mínimo, definido como a restrição de direitos e permissões de acesso para usuários, contas, aplicativos, sistemas, dispositivos (como os de Internet das Coisas – IoT) e processos de computação ao mínimo necessário para executar as atividades rotineiras e autorizadas.

O uso de uma solução robusta PAM oferece vários benefícios, incluindo:

1. redução da superfície de ataque: a limitação de privilégios para pessoas, processos e aplicativos reduz significativamente os caminhos e entradas para exploração;

2. redução da capacidade de propagação de *malware*: muitas variedades de *malware* precisam de privilégios elevados para instalar ou executar. A remoção ou limitação de privilégios, como por meio da imposição de política de privilégios mínimos em toda a organização, torna mais difícil para um *malware* se instalar ou realizar automaticamente as ações de movimento lateral, infectando outros dispositivos da rede;

3. incremento do desempenho operacional: a restrição de privilégios ao grupo mínimo de processos necessários para executar uma atividade autorizada reduz a chance de problemas de compatibilidade entre aplicativos ou sistemas e ajuda a reduzir o risco de tempo de inatividade;

4. redução da complexidade do processo de conformidade: a restrição das atividades privilegiadas que podem ser executadas ajuda a criar um ambiente menos complexo e, portanto, mais amigável para auditoria;

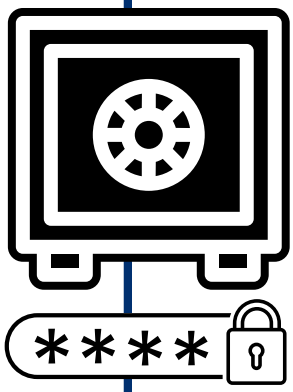
5. favorece a implementação da autenticação multifator (MFA) para todos os administradores do sistema: isso evita que apenas descobrir a senha de um administrador permita o acesso aos recursos do sistema;

6. favorece o acesso *Just-In-Time* (JIT): uma solução robusta PAM garante a implantação do “Princípio do Privilégio Mínimo (PoLP)” e reforça a abordagem de acesso *Just-In-Time* (JIT). O JIT é uma prática de segurança fundamental em que o privilégio concedido para acessar aplicativos ou sistemas é limitado a períodos de tempo predeterminados, conforme a necessidade. Isso ajuda a minimizar o risco de privilégios permanentes, num esquema 24x7, que invasores ou pessoas mal-intencionadas podem explorar prontamente;

Componentes-chave da Gestão de Acesso Privilegiado (PAM)

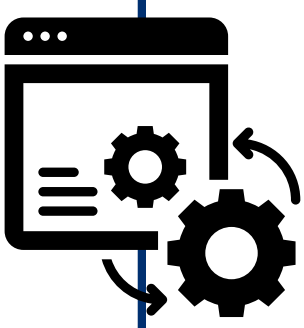
Uma solução PAM é um mecanismo de segurança composto por diversos componentes (vide Figura 1). Dependendo das necessidades de segurança do ambiente, a solução PAM envolverá diferentes processos e tecnologias, a saber:

Gestão de Contas Privilegiadas: refere-se aos mecanismos que gerenciam e auditam contas que têm acesso ao sistema com privilégios além daqueles do usuário padrão. Em alguns sistemas PAM, a Gestão de Contas Privilegiadas refere-se à tecnologia que armazena credenciais de contas privilegiadas (como suas senhas) em um cofre de senhas especial e altamente seguro. Além de armazenar as credenciais, ela também pode impor políticas sobre as suas condições de acesso como, por exemplo, exigir que usuários que necessitam de acesso a uma conta de serviço privilegiada que executa um sistema crítico utilizem um mecanismo de autenticação exclusivo. Em algumas instâncias, um portal de gestão de contas privilegiadas pode alterar automaticamente a senha no cofre e no sistema, garantindo que as credenciais permaneçam seguras após terem sido acessadas;



Gestão de Sessão Privilegiada (PSM): é um componente de uma solução PAM que permite aos administradores monitorar, gerenciar e auditar as atividades de usuários privilegiados. Ele rastreia e registra sessões iniciadas por usuários internos, usuários externos e sistemas conectados com privilégios acima daqueles de um usuário padrão. Essas soluções reduzem o risco de incidentes através da notificação, em tempo real, aos administradores de segurança sobre quaisquer atividades anômalas que envolvam uma conta privilegiada, permitindo que sejam encerradas caso se desconfie que esteja ocorrendo uma atividade maliciosa. Ao usar uma solução PAM que suporta gerenciamento de sessão privilegiada, também é possível registrar sessões privilegiadas para análise futura;

descoberta automatizada: a maioria das organizações tem milhares de contas, endpoints e credenciais privilegiadas, e é impossível descobrir e integrar todas elas manualmente. Uma solução PAM precisa permitir descobrir automaticamente contas e recursos privilegiados em massa e gerenciá-los a partir de um único painel centralizado. Além disso, ela também deve permitir descobrir automaticamente os serviços, pontos de extremidade e credenciais associados às contas e recursos descobertos;



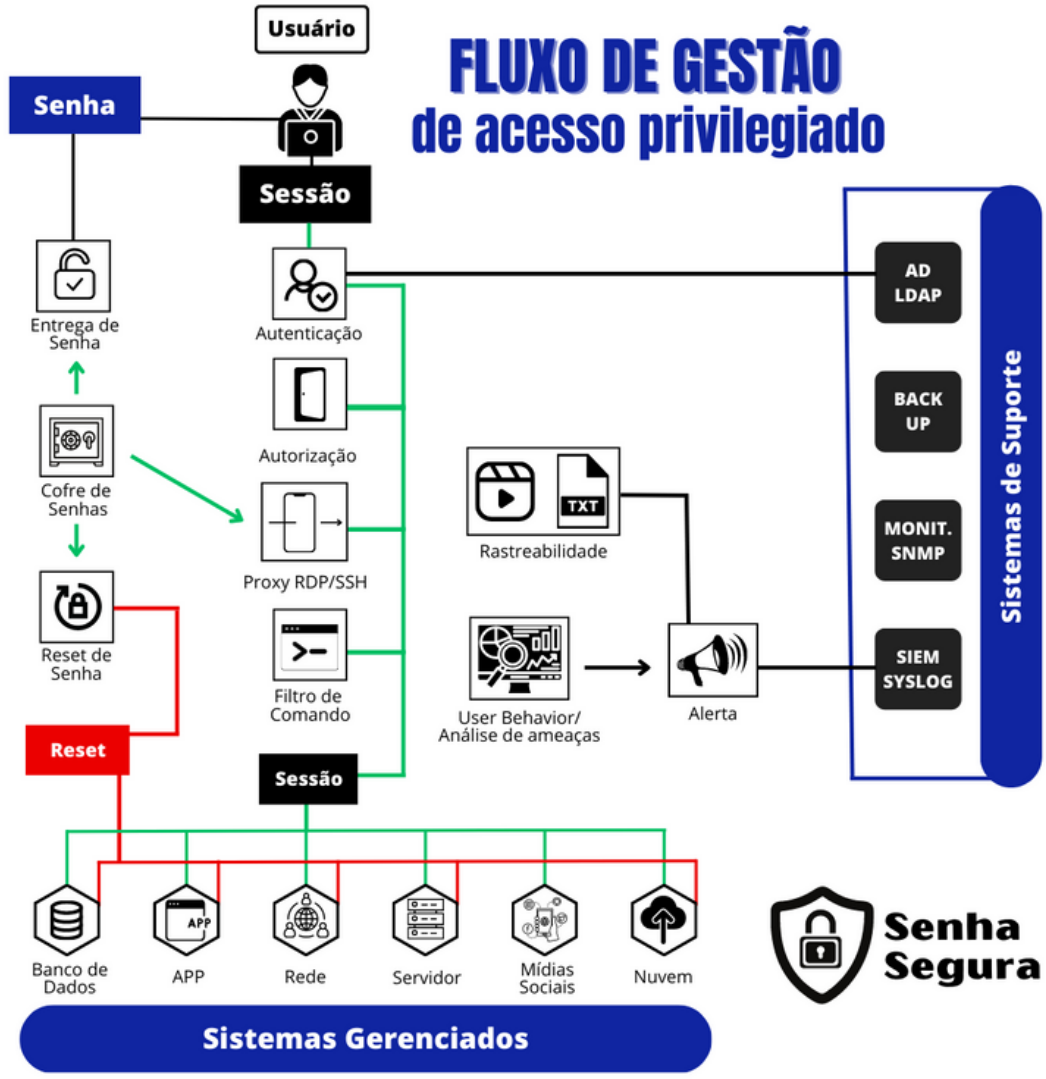
Gestão de Elevação de Delegação de Privilégios (PEDM): conceder aos usuários privilégios mais altos e acesso permanente a contas privilegiadas apresenta riscos de segurança significativos. Esses privilégios permanentes dão aos invasores acesso aos recursos mais valiosos de uma organização. A PEDM em soluções PAM visa resolver esse problema, permitindo que usuários e aplicativos acessem informações privilegiadas usando uma abordagem baseada em tempo e solicitação. Em outras palavras, o acesso a informações sensíveis é dado por um tempo estipulado com base na validação dos requisitos do usuário, e esses privilégios são revogados após esse tempo. Com efeito, a PEDM permite que as equipes de TI implementem o Princípio do Privilégio Mínimo (PoPL), no qual se fornecem apenas privilégios suficientes para que os usuários executem seus trabalhos apenas quando necessário, o que elimina os riscos de privilégios permanentes associados a contas privilegiadas não gerenciadas, desatualizadas e órfãs; e

auditoria em tempo real: O registro de auditoria de uma sessão privilegiada inclui qual foi o evento, qual usuário ou aplicativo iniciou o evento (incluindo o endereço IP e o tipo de dispositivo), quais operações foram executadas durante toda a sessão e a data e hora do evento. As trilhas de auditoria criam responsabilidade para cada ação, garantindo que atividades suspeitas e falhas do sistema possam ser rastreadas para entender suas origens. Além disso, a manutenção de trilhas de auditoria para acesso privilegiado é um componente dos padrões de conformidade em segurança da informação, que esperam que as organizações monitorem e capturem todas as ações executadas por contas privilegiadas (norma ABNT NBR ISO/IEC 27002:2005, item 10.10.2, Monitoramento do uso do sistema, dentre outras).

Informações complementares

1. **Cultura *DevOps*:** cultura *DevOps* é um conjunto de práticas e valores que visam a colaboração, integração e comunicação entre as equipes de desenvolvimento de software e de operações de TI, com o objetivo de melhorar a entrega de software e a qualidade do serviço prestado aos usuários finais. É baseada em uma filosofia de trabalho ágil e iterativa que enfatiza a automação e a melhoria contínua de todo o processo de desenvolvimento, teste e implantação de *software*.
2. **Chaves SSH:** Uma chave SSH é um par de chaves criptográficas que é usado para autenticação e criptografia em conexões SSH (*Secure Shell*), um protocolo de rede seguro que é comumente usado para acessar servidores remotos e transferir arquivos de forma segura. A chave SSH é composta de uma chave privada e uma chave pública. A chave privada é mantida pelo usuário em seu próprio computador e é usada para descriptografar mensagens criptografadas com a chave pública correspondente. A chave pública, por sua vez, é armazenada no servidor remoto e é usada pelo cliente SSH para criptografar mensagens antes de enviá-las para o servidor.

Figura 1



O Departamento de Segurança da Informação e Cibernética (DSIC) recomenda aos usuários que:

- incluam em suas políticas a implementação do princípio do mínimo privilégio;
- configurem corretamente seus aplicativos com critérios de segurança, inclusive o MFA, que protejam a privacidade, a integridade e a disponibilidade; e
- ao identificar um incidente cibernético em sua organização informe imediatamente à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) de sua instituição.

O DSIC orienta aos integrantes da administração pública federal observar o previsto no Plano de Gestão de Incidentes Cibernéticos, particularmente quanto à prevenção. Ele está disponível em:

https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/plano-de-gestao-de-incidentes-ciberneticos-plangic/plangic.pdf

Na segunda e última parte desta OSIC daremos mais recomendações com maior detalhamento.

Por fim, o DSIC solicita, ainda, que propostas de temas, sugestões ou outras contribuições sejam encaminhadas ao e-mail educa.si@presidencia.gov.br para fomentar futuras emissões de OSICs.

TLP:CLEAR